b·ccentre

BELGIAN CYBERCRIME CENTRE OF EXCELLENCE
FOR TRAINING, RESEARCH & EDUCATION

LEGAL RESEARCH REPORT

With the financial support from the Prevention of
and Fight against Crime Programme of the European Union
European Commission – Directorate-General Home Affairs

b·ccentre
BELGIAN CYBERCRIME CENTRE OF EXCELLENCE
FOR TRAINING, RESEARCH & EDUCATION

2011 – 2014

Research Report
Legal

With the financial support from the Prevention of and Fight against Crime Programme of the European Union
European Commission – Directorate-General Home Affairs

With the financial support from the Prevention of and Fight against Crime Programme of the European Union
European Commission – Directorate-General Home Affairs

With the financial support from the Prevention of and Fight against Crime Programme of the European Union
European Commission – Directorate-General Home Affairs

With the financial support from the Prevention of and Fight against Crime Programme of the European Union
European Commission – Directorate-General Home Affairs

b·ccentre
BELGIAN CYBERCRIME CENTRE OF EXCELLENCE FOR TRAINING, RESEARCH & EDUCATION

Foreword

The Belgian Cybercrime Centre of Excellence for Training, Research and Education is Belgium's central coordination, collaboration and knowledge sharing platform in the fight against cybercrime. B-CCENTRE coordinates research teams at various universities which collaborate across disciplines on specific cybercrime, cybersecurity and cyberforensics related topics in both fundamental and applied research activities. Together with experts from public sector and industry partners, the academic B-CCENTRE partners design and teach basic and advanced trainings on specific cybercrime topics and develop and implement awareness raising initiatives in Belgium. B-CCENTRE does not only focus its efforts on a national level, but engages in the fight against cybercrime beyond the Belgian borders through numerous contacts with similar centres abroad. B-CCENTRE is the Belgian node in the European network of Cybercrime Centres of Excellence and collaborates with the main European and international organisations dealing with cybercrime. It is sponsored by the Prevention of and Fight against Crime Programme of the European Union, under contract HOME/2010/ISEC/AG/INT-011, and co-funded by the academic partners, under the coordination of the KU Leuven.

The B-CCENTRE started its activities in spring 2011 and has since launched and supported numerous activities to enhance knowledge and knowledge sharing related to cybercrime, digital forensics, cybersecurity, online behaviour and risks, privacy, data protection and other related topics in Belgium and beyond. This book provides an overview of the results of the legal research performed in the frame of the EU sponsored B-CCENTRE project, 18 April 2011-17 November 2014. There is a similar publication on the results of the criminological and of the technical research performed. These three publications are complementary to the B-CCENTRE report of activities.

For further reading we refer to the publications section under the research tab on our website, www.b-ccentre.be, where you can find the links to the published articles of which the abstracts are included in this publication. On the site you can also find information about B-CCENTRE partners and activities as well as an overview of relevant actors, education programmes and awareness raising activities in Belgium and other interesting leads.

We wish you an interesting read and welcome your feedback on the work done.

Ann MENNENS
Manager B-CCENTRE
KU Leuven – iMinds – ICRI/CIR
Sint-Michielsstraat 6, box 3443, BE-3000 Leuven
ann.mennens@b-ccentre.be
www.b-ccentre.be
@B_CCENTRE

With the financial support from the Prevention of and Fight against Crime Programme of the European Union
European Commission – Directorate-General Home Affairs

Executive Summary

Overview

In the B-CCENTRE Project, Work package 3 deals with the legal aspects of cybercrime. It is devoted to fundamental and applied scientific research and the development and organisation of advanced training courses in the law discipline.

The three main legal research topics defined in the project relate to:

- The purpose specification principle in the Area of Freedom, Security and Justice (L1)
- Taxonomy and legal impact of illegal conduct and content risks for minors on social network sites (SNS) (L2)
- Adaptation of the Belgian criminal law and procedures to specificities of the cybercontext (L3)

Furthermore, a series of advanced legal cybercrime training modules were planned in English/Dutch (L4) and French (L5).

The objectives set have largely been met since additional study work has been performed by the dedicated research teams, including also researchers funded on other than B-CCENTRE resources. Activities have resulted in a Legal Research Report, several published articles, legal education and training modules and have been presented at different conferences, seminars and training sessions[1].

Themes covered

The legal research developed in the frame of the B-CCENTRE project builds further on research lines already started at the respective departments, namely privacy and data protection, online investigations and evidence gathering. The expertise developed by the KU Leuven Research Departments ICRI and The Institute of Criminal Law as well as UNamur's CRIDS former to the project start, were one of the reasons why these research institutes have played a key role in the development of the project.

Stimulated by the B-CCENTRE environment and resources, research focussed in the past three years and a half specifically on cybercrime and on topics of relevance for law enforcement dealing with it on a daily basis, be it police or magistrates.

The use of cyberspace and the challenges related to it are evolving rapidly thanks to fast changes in the technology and tools used. Improvements and changes and with them new challenges and dangers occur at increasing speed. Considering the fast evolution of the research matter, it was not possible to foresee all the legal implications that needed to be studied further related to the technological changes. In the course of the project additional research was therefore performed and presented in articles and at the B-CCENTRE seminars and conferences.

Still, the two main legal challenges in the fight against cybercrime in Belgium centre around

- the trade-off between ensuring a high level of security for citizens and preserving their fundamental rights, such as the right to privacy.
- The interpretation of the existing legal basis for application in the virtual world, for preventive and repressive measures and actions

[1] Most information on these activities is available on the B-CCENTRE website – www.b-ccentre.be.

With the financial support from the Prevention of and Fight against Crime Programme of the European Union
European Commission – Directorate-General Home Affairs

These topics are studied in detail by ICRI when looking into the use of technical applications that can be employed for improving (physical) security, identity management, enhancing a safer internet experience, prevention, discovery and stopping of malicious attacks. Research includes the purpose specification, modalities for blocking illegal content, the modalities for use of information sharing platforms, legal basis for crawling and monitoring (anti-botnet), privacy and data protection issues related to biometric applications and the need to avoid spoofing, identity theft on social media, data breach notification and accountability of surveillance practices. Specific attention has also been given to the particular situation of children on SNS, both as a user and as a victim. The EU approach towards cybersecurity has been studied and an analysis was made of the EU guidelines in the field of cybersecurity.

The KU Leuven Institute of Criminal Law centred its research around three general topics: the *substantive criminal* law on cybercrime, criminal *investigative measures* in a digitalised environment and *jurisdictional* issues related to the cross-border nature of cyber investigation.

Many of the publications are in Dutch. This was a deliberate choice. Although from an academic perspective this might have been less 'lucrative' for the individual researchers, it was a deliberate choice not to preach to the converted, but to target on purpose a broader Belgian audience of practitioners, local decision makers and scholars to raise awareness as to the possibilities, challenges and compatibility discussions at the crossroads of Belgian, supranational and international law. The B-CCENTRE allowed however to have some of the Dutch texts translated into English, as the stakes of the debate go beyond the specific Belgian situation and the same legal issues will arise all over the world.

The publications on substantive criminal law analyse the implementation of traditional and new IT-specific legal provisions in practice. Several provisions in the current legal framework were found wanting as to their compatibility with the 'online = offline – principle', which the Belgian government and parliament takes as the basis of their legislative policy. The incoherent approach which the Belgian parliament has towards the traditional criminal offence of 'document' forgery and new IT-forgery provides a good illustration.

The publications on criminal investigative measures focus on the implementation of the existing Belgian legal framework in the specific context of cyber investigative practice, and more particular in the context of social media as a source for evidence gathering. The current outdated framework poses many difficulties, which necessitates research to find workable and 'human rights - proof' solutions.

One particular issue thoroughly investigated is the problem of territorial jurisdiction in the context of search and seizure of data. In contrast to traditional physical criminal evidence, digital evidence is linked to several territories resulting in anomalies with regard to the application of the well-established territoriality principle as the leading criterion shaping jurisdiction. These research results are published in this report. A similar jurisdictional problem arises when the cooperation of internet service providers is ordered.

The multi-sector and multi-disciplinary approach

The enhanced cooperation of the academic researchers with experts from public and private sector in the framework of the B-CCENTRE project has substantially increased the societal relevance of the research and opened up some new ways of reflection.

The non-disclosure agreement signed by all academic partners reinforced the needed **trust** relation for exchange of sometimes sensitive information and increased cooperation amongst partners from different sectors. It also opened up the possibility of involving academics in some of the thinking regarding the challenges law enforcement is confronted with on a daily basis in the application of the existing legal basis, be it Belgian or European.

With the financial support from the Prevention of and Fight against Crime Programme of the European Union
European Commission – Directorate-General Home Affairs

The multi-disciplinary approach taken for the implementation of the B-CCENTRE project ensured that measures taken on a legal level would be technically viable and vice versa. The co-operation with IT-experts is important, both for a better understanding of the possibilities of law enforcement and for the limitations.

A multi-disciplinary view is also provided in the Cybercrime training for magistrates, as well as in the cybercrime education developed at Master and LLM level. Several experts are invited to provide their insights and knowledge to the legal community and discuss with them the implications this could have on the work of the legal experts.

European cooperation

B-CCENTRE has substantially stimulated exchanges with scholars and experts in other countries, thanks to the subsidies provided for organising exchanges with academic peers from other countries, in the EU and worldwide and for participation to conferences, seminars and workshops organised in Europe and beyond. This provided excellent food for thought for the research performed but also an occasion and platform for sharing expertise and research results.

In particular results have been shared with the other Cybercrime Centres of Excellence, by inviting them as participants and as speakers at B-CCENTRE seminars and conferences, by sharing insights and results at meetings of the 2CENTRE network (e.g. CyNC in Dublin in December 2013) and making it available on the dedicated 2CENTRE platform on the Europol Platform for Experts (EPE)

Most of the work done has been reflected in articles published and in training material made available in the different seminars and workshops, involving actors from public and private sector. All of this is made available via the website and the research results are bundled in the B-CCENTRE Legal Research Report. This material is publicly available to interested parties.

B-CCENTRE impact

After three years and 7 months of B-CCENTRE activity in the legal area, a number of changes have occurred in the Belgian landscape. Partners have got to know each other much better and a trust relation has been established between different actors, like e.g. academics, Police, Magistrates, State Security, Defence, Data Protection Authority (DPA). This results in increased knowledge exchange and cooperation, and also positively impacts the level of the education and training provided, e.g. training provided to magistrates and magistrates to be: introduction of new courses related to cybercrime and improvement of courses thanks to the knowledge gained, and involvement of field experts in provision of education thanks to the network established. The number of experts who are knowledgeable in cybercrime related legal matters has increased substantially and more and more specialised cybercrime magistrates are being formed.

Overall there is an increased expertise and knowledge in Belgium on the legal aspects of dealing with cybercrime, and a circle of trust has been established between actors.

As to the Institute of Criminal Law, the B-CCENTRE has brought new impulses in the field of cybercrime (co-operation with African countries, the peculiar situation of working with Russia), which was an incentive to support other research in this field: a Malawi scholar is conducting research on co-operation of law

With the financial support from the Prevention of and Fight against Crime Programme of the European Union
European Commission – Directorate-General Home Affairs

enforcement with the private sector in Africa, an Erasmus Mundus PhD researcher from the University of Kazan (Russia) on the procedural guarantees regarding digital evidence, is working with us this year.

Overall, the co-operation within the B-CCENTRE has mainly strengthened the personal links with people or institutions which the academic actors often knew by name or publications, but who are now partners or potential partners for future research.

Possible policy recommendations at Belgian/EU level

Though very much referring to legal-technical issues, all publications made in cooperation with B-CCENTRE contain policy oriented suggestions. Input from and exchanges with the Federal Computer Crime Unit (FCCU), prosecutors and judges, helped the researchers to understand the urgency of certain issues and gave them insight into the practical concerns underlying innovative interpretations of the law or technical problems. The exchanges often provided for more layered and nuanced approaches to the issues, although as independent academics, we sometimes disagreed with some of the project partners on international law or human rights issues.

The impact on case law and future legislation is hard to assess, but as a major reform of the Belgian Code of Criminal Procedure is envisaged, it is likely that the publications and their authors will be taken into account when it comes to general policy theories, like the one on geo-localisation of investigative action on the Internet.

The way forward

The B-CCENTRE project has provided a strong energy boost for legal cybercrime related research in the participating legal research departments but also to peer research institutes in Belgium and beyond. The PhD work started under the project will be continued and delivered in the coming years resulting in new substantiated views on cybercrime related legal work. Several publications and presentations on the topics researched will be made available to a wider audience.

New research will be and has already been defined to continue on the basis set by the B-CCENTRE project. Seminars and conferences will be organised to keep up to date with the fast upcoming changes in the digital world. The sessions organised in the course of the B-CCENTRE showed that there is a keen interest in the topics and that there is a need for continuation and enhancement of the training and education modules developed as well as of the possibilities for knowledge exchange.

Through participation in the Belgian Cyber Security Coalition the research members hope to continue to supply their research finding to people in practice, disseminate them to different target audiences and receive impulses for further legal research.

With the financial support from the Prevention of and Fight against Crime Programme of the European Union
European Commission – Directorate-General Home Affairs

Partners

Applicant organisation/Coordinator

KU Leuven

KU Leuven is the largest academic institution in Belgium and one of the oldest European universities as it was founded in 1425. It is a research-intensive, internationally oriented university that carries out both fundamental and applied research. It is strongly inter- and multidisciplinary in focus and strives for international excellence. To this end, KU Leuven works together actively with its research partners at home and abroad.

With a research expenditure of € 365 million in 2012, the KU Leuven is a leading research university in Europe. KU Leuven is also a member of the League of European Research Universities (LERU), a group of twenty European research-intensive universities committed to the values of high-quality education in an internationally competitive research environment. More than 200 KU Leuven researchers are permanently working on information and communications technology related issues. They belong to different university departments with a strong tradition in multidisciplinary research on information and communications technology issues.

The Interdisciplinary Centre for Law & ICT - ICRI

ICRI is co-ordinating the activities of the Belgian Cybercrime Centre of Excellence for Training, Research and Education - B-CCENTRE.

The Interdisciplinary Centre for Law & ICT (www.icri.be) is a research centre at the Faculty of Law of KU Leuven dedicated to advance and promote legal knowledge about the information society through research and teaching of the highest quality. ICRI is among the founding members of the LEUVEN Centre on Information and Communication Technology (LICT) and the Flemish ICT Research Institute iMinds. Currently, ICRI is part of the iMinds Security Department, a de facto "one-stop-shop for ICT security research".
ICRI is committed to contribute to a better and more efficient regulatory and policy framework for information & communication technologies (ICTs). Its research is focused on the design of innovative legal engineering techniques and is characterised by its intra- and interdisciplinary approach, constantly aspiring cross-fertilisation between legal, technical, economic and socio-cultural perspectives. By conducting ground-breaking legal research in a spirit of academic freedom and freedom of inquiry, ICRI aspires to a place among the centres of excellence in the area of law & ICT in Europe and beyond.

As from 1 July 2014 ICRI merged with the Leuven Centre of Intellectual Property Rights (CIR) with which it has been collaborating for several years. The full integration of complementary expertise will enable the new research unit to expand its mission and vision in future research and teaching activities.

Institute of Criminal Law

The Institute of Criminal Law was founded in 1983 as a separate Institute within the Research Unit Criminal Law and Criminology in the Faculty of Law of the KU Leuven. The specificity of criminal law as a legal branch and its technical-legal idiosyncrasies require specialisation. This does not imply, however, that the staff of the Institute would lock itself up in its own field. On the contrary: criminal law often sanctions violations in other areas of the law. Furthermore criminal procedures, intended to result in criminal sanctions, usually function alongside or together with other formal or informal sanctioning mechanisms. That is why criminal law scholars are ideal partners for all kinds of interdisciplinary cooperation.

Without ignoring general knowledge and practice, the Institute's staff specialises in research on Terrorism and organised crime, White collar crime (in particular Cybercrime), Criminal procedure and evidence gathering in a digital world, Protection Mechanisms in Criminal Procedure, Sentencing and the Execution of Sanctions. Within each area there is continuous concern for the interplay between national and international (particularly European) norms and policies on the one hand and between substantive law and procedure on the other.

The research of the Institute related to cybercrime, digital evidence and investigative measures in a digitised world focuses on the current substantive and procedural legal framework. It looks for shortcomings and anomalies and aims to make suggestions for improvement. It analyses the legal possibilities of detecting, prosecuting and punishing criminal activities in our digital information society and investigates the procedural requirements of digital evidence gathering. It also looks into the international cooperation, in particular regarding the jurisdictional issues related to digital evidence gathering.

Co-beneficiaries

University of Namur (UNamur)

Former Facultés Universitaires Notre-Dame de la Paix (FUNDP)

CRIDS

The Research Centre on Information, Law and Society (CRIDS) at the University of Namur brings together more than fourty senior and junior researchers to address questions relating to information systems and technological choices that match the ethical requirements of a human life. This includes a large scope of issues, from the protection of digital consumers or patients to the privacy protection, from new modes of governance to the production of common cultural goods, from electronic communication law to issues raised by systems of profiling and personalisation but also questions raised by the fight against cybercrime and the protection of IT security. The mission statement of CRIDS is to lead applied and fundamental researches with a critical regard and a permanent care for the democratic and human values. CRIDS is and has been involved in several FP6 and FP7 projects. It is in charge of many national and regional R&D project and has been awarded by the Belgian Science Policy Office for the quality of its research.

Manager

Ann Mennens

Ann Mennens is the Manager of the B-CCENTRE Project. She started working in September 2011 at ICRI, KU Leuven to organise the work of the Belgian Cybercrime Centre of Excellence for Training, Research and Education. She coordinates the activities of several academic research groups, public sector bodies and businesses in Belgium dealing with cybercrime. She initiates, supports and manages interdisciplinary research on cybercrime and cyber security, the development and teaching of basic and advanced cybercrime trainings. She is active in setting up and creating awareness raising initiatives related to safe online experiences, both for businesses and organisations, as well as the general public. She is representing the B-CCENTRE in conferences and working groups in Belgium, the EU and worldwide.

She is one of the founding members of the Belgian Cyber Security Coalition, a coalition of public authorities, the academic world and the business sector joining forces against cybercrime in Belgium. It brings together more than 50 key players to share knowledge, raise awareness among citizens and businesses and issue recommendations for a more efficient policy. www.cybersecuritycoalition.be

For over 20 years, she has led various projects in the field of Justice and Security, involving governmental and other actors from the EU Member States and beyond. The fight against crime and cooperation between judicial authorities and law enforcement in the EU, have been at the core of the projects under her management. She has a track record of creating networks and systems for cooperation, information exchange and dissemination and of organising training programmes for several target groups, in particular Police and Judiciary.

Professors

Prof. Dr. Jos Dumortier

Jos Dumortier is Professor-emeritus of ICT Law at the University of Leuven (www.kuleuven.be), Director of the Interdisciplinary Research Centre for ICT and Law (ICRI) (www.icri.be) from 1990 till 2014 and Research Leader in the iMinds Security Department (www.iminds.be) until 2014. With his research team he participated in a series of European and national ICT-related R & D projects in particular in the areas of privacy and identity management, information security and e-business. He is the co-founder of the B-CCENTRE (www.b-ccentre.be) which he headed for more than three years. Jos Dumortier is a member of the Bar of Brussels and partner in "time.lex", a law firm specialised in information and technology law (www.timelex.eu). He participates in the boards of several national and international scientific and business associations and is a member of various editorial and program committees. He is the editor of the International Encyclopedia of Cyber Law and the author of more than one hundred books and articles on legal issues related to the information society.

Prof. Dr. Frank Verbruggen

Frank Verbruggen is Professor at the Institute of Criminal Law of the KU Leuven, Belgium. He teaches Criminal Law, the Law of Criminal Sanctions, European Criminal Law and International Criminal Law. He set up the course on 'Cybercrime and Crime Control in a Digitising World' in the master programme of the Law Faculty[1]. He is a guest professor (Belgian) Criminal Law and Procedure at the University of Hasselt.

He has studied the impact of the fight against organised crime and terrorism on criminal law and procedure. His current research focuses on pan-European principles legitimising and limiting mutual recognition in criminal matters and legal aspects of the fight against cybercrime, particularly its impact on law enforcement's investigative powers, international cooperation and evidence law. He also is a lawyer at the Leuven Bar, as *of counsel* with Lovius.

Yves Poullet

Yves Poullet has been the director of CRIDS since its creation in 1979 until August 31, 2010. He conducted various researches in the field of new technologies with a special emphasis on privacy issues, of individual and public freedom in the Information Society and of Internet Governance. Moreover, he is full professor at the Faculty of Law at the University of Namur (UNamur) and Liège (Ulg).

He has been during 12 years (1992-2004) member of the Belgian Commission on Data Protection (Commission belge de protection de la vie privée). In addition, he was since its origin, member of the Legal Advisory Board of the European Commission and the president of the Task Force "Electronic Democracy and Access to public records". He is a founder of the European Telecommunication Forum, ECLIP and FIRILITE. He also chaired the Belgian Computer Association ABDI (Association Belge de Droit de l'Informatique).

[1] This course has been taught for the first time in the academic year 2013-14 in Dutch. It will be lectured in an English language version by prof. Panzavolta from 2014 onwards.

Researchers

Charlotte Conings

Charlotte Conings studied law (specialisation criminal law) at the Law Faculty of the University of Leuven, from which she graduated in June 2011. She participated in the Erasmus exchange programme and spent half a year in Montpellier, France, studying at Université Montpellier I. Since September 2011 she is a PhD candidate at the Institute for Criminal Law of the University of Leuven and an affiliated researcher at the B-CCENTRE.

Under the supervision of Prof. dr. Frank Verbruggen, Charlotte is preparing a PhD on the criminal procedure regime for search in the physical and digital world. She published several articles and gave presentations at national and international conferences on topics related to her research such as computer searches, criminal investigation and social media, remote searches in the cloud, the duty to decrypt and hacking by law enforcement. Within the framework of the B-CCENTRE, she has co-organised the expert seminars concerning online criminal investigations and intrusive methods of cyber investigation. She further co-organised two legal advanced trainings concerning criminal investigation with regard to social media platforms.

Fanny Coudert

Fanny Coudert obtained her law degree in French and Spanish law in 2000 at the Université Panthéon–Sorbonne in Paris and University Complutense of Madrid (maîtrise en droit integrée français et espagnol). In 2001, she obtained a Master degree in ICT Law (special award for dissertation) at the University Complutense de Madrid, and in 2004, she obtained a pre-doctorate degree (D.E.A) at the same University (Magna Cum Laude). During her doctorate training studies, she worked as a data protection auditor, and as an in-house lawyer in a consumer organisation. She is a member of the Madrid Bar Association since 2001.

In July 2006 Fanny joined ICRI where she conducts research in the field of privacy. She is preparing a PhD on the topic of "The purpose specification principle in the Area of Freedom, Security and Justice: towards renewed data protection principles for information-based practices in the field of Security" under the supervision of Prof. Dr. J. Dumortier and Prof. Dr. F. Verbruggen. She currently focuses on the principle of accountability and privacy by design in the context of surveillance through her participation to two FP7 EU projects PARIS (PrivAcy pReserving Infrastructure for Surveillance) and PRIPARE where she focuses on the development of training courses on the concept of privacy-by-design. She previously conducted research on privacy and virtual worlds within the FP7 project +Spaces (Policy Simulation in Virtual Worlds), privacy and video surveillance within the FP7 EU project SCOVIS (Self-Configurable Cognitive Video Supervision) and the EU FP6 projects DYVINE (Dynamic visual networks), in Belgian projects such as FLEXYS (Flexible Traffic Management) or SPAMM (Solutions Platform for Advanced Mobile Mesh). She also worked on privacy and biometrics, location data, ID theft and forensic/risk profiling (Network of Excellence FIDIS - Future of Identity in the Information Society and TURBINE).

Kristel De Schepper

Kristel De Schepper studied law at the Law Faculty of the University of Leuven and the Université Robert Schuman in Strasbourg (Erasmus exchange programme). After obtaining her law degree in 2006, she practiced law at the Antwerp bar for five years. She first joined the Institute of Criminal Law as a teaching assistant in 2008, later in 2010 she became a researcher. Her research interests are cybercrime, white collar crime and criminal investigation in a digital society.

Within the framework of the B-CCENTRE, she has co-organised the legal expert seminars concerning online criminal investigations and intrusive methods of cyber investigation and conducted research in the field of substantive criminal law issues related to cybercrime. She is preparing a PhD entitled "Criminalisation of espionage and information abuse to protect business secrets" under the supervision of Prof. Dr. Frank Verbruggen. In general, she examines whether our (Belgian) substantive criminal law is up to the challenges of the information society. On the basis of a case study of the criminalisation of economic espionage, the research intends to establish criteria which should guide lawmakers considering the use of criminal law in our digital information society. She also participates in the FP7 EU project EKSISTENZ (Harmonised framework allowing a sustainable and robust identity for European Citizens) where she conducts research on criminal law measures to combat identity theft.

Karel Demeyer

Karel Demeyer obtained a Master's degree in both Criminological Sciences and Applied Computer Sciences. At ICRI, he was part of the team setting up the B-CCENTRE (Belgian Cybercrime Centre of Excellence for Training, Research & Education). He joined in September 2011 The Leuven Institute for Criminology (Catholic University of Leuven) until 2013. During his time at ICRI he was concerned with the research design of the B-CCENTRE project and contributed to the legal research. Karel has now joined the Belgian Federal Police and will start working in the Federal Computer Crime Unit (FCCU).

Franck Dumortier

Franck Dumortier has a degree in law and a post-graduate diploma in law and management in communication and information technologies. He is assistant teacher and senior researcher at the Information Technology, Law and Society Research Centre (CRIDS) at the University of Namur since 2005. His research particularly focuses on the impact of technologies such as RFIDs, biometrics, surveillance cameras and online social networks on the fundamental human right to privacy. His researches also cover the field of cybercrime legislation. He participated in numerous national and European projects and published numerous articles in those research fields.

Karine e Silva

Karine e Silva (LL.M.) is a legal researcher at the Belgian Cybercrime Centre of Excellence for Training, Research and Education (B-CCENTRE) within the Interdisciplinary Centre for Law and ICT (ICRI) at the Katholieke Universiteit Leuven (KUL) since March 2013. She investigates data privacy issues in the implementation of cybercrime mitigation tools in the frame of the EU Advanced Cyber Defence Centre (ACDC) project and information sharing networks on the protection of critical infrastructure in the European Control System Security Incident Analysis Network (ECOSSIAN) project. Her interests lie in the promotion of multistakeholder approaches to cyber security and the development of international public-private partnerships against cyber incidents.

Catherine Forget

Catherine Forget has a degree in law and a post-graduate diploma in social law. She is researcher at the Information Technology, Law and Society Research Centre (CRIDS) at the University of Namur since 2014. She is lawyer since 2014. Her research particularly focuses on the impact of technologies on the fundamental human right to privacy. Her researches also cover the field of cybercrime legislation.

Claire Gayrel

Claire Gayrel worked a period for the European Regional Development Found (ERDF) in French Guyana, before joining the CRID in September 2008. She graduated in European Law and political sciences. Her researches currently focus on transborder data flows and on the protection of personal data in the Justice, liberty and security area of the European Union.

Els Kindt

Dr. Els Kindt is a post-doc legal researcher at the Center for Law and ICT (ICRI) at the Law Faculty of the KU Leuven, Belgium. She graduated in law in 1987 at the KU Leuven and obtained a Master of Laws (LL.M) in 1988 in the United States. Her research focuses on privacy and identity management and includes in-depth research of the legal aspects of biometric data processing. She participated as principal legal researcher in various national and EU projects, including B-CCENTRE. Before joining ICRI, she practised law as an IP and ICT law attorney in an international law firm in Brussels. She is a frequent speaker at international events and has published several articles on recent developments in IT law, has been invited as expert, is lecturer on European privacy and data protection and electronic contracts and is member of the editorial board of 'Computerrecht' and 'Privacy en Informatie'. Her Ph.D was on legal aspects of biometric data processing. She is a member of the Belgian national Privacy Commission (Replacing member - National Registry Committee - 2014-2020).

Eva Lievens

Eva Lievens holds a law degree from the University of Ghent (2002), a Masters degree in Transnational Communications and Global Media from Goldsmiths College, London (2003) and a Phd in Law from KU Leuven (2009). She has been a member of the Interdisciplinary Centre for Law & ICT (www.icri.be) since 2003 and is currently a Postdoctoral Research Fellow of the Research Fund Flanders, working on a project titled 'Risk-reducing regulatory strategies for illegal and harmful conduct and content in online social network sites'. Her research focuses on legal challenges posed by new media phenomena, such as the regulation of audiovisual media services, user-generated content and social networks, with a specific focus on the protection of minors and fundamental rights. She has also been involved in the creation of the B-CCENTRE (Belgian Cybercrime Centre of Excellence for Training, Research & Education). Eva is a member of the Advisory Committee of the BE SIC II-project (EU Safer Internet Programme) and the Belgian Film Evaluation Committee, and is the Associate Editor of the International Encyclopaedia of Laws – Media Law (edited by Prof. dr. Peggy Valcke). She is the Programme Coordinator of the Masters in Intellectual Property Rights and ICT Law, in which she teaches the course Public Government & Cybercrime Law, and a Guest Professor at Ghent University, where she teaches Media Law and Copyright Law.

Ruben Roex

Ruben Roex is a legal researcher at the Interdisciplinary Centre for Law and ICT at KU Leuven. After obtaining his master's degree in economics, law and business administration (2009) as well as his master's degree in law (2011), he worked almost 3 years for the Belgian Cybercrime Centre of Excellence for Training, Research and Education. During this time, he worked on a wide range of legal topics in the areas of cybercrime and cybersecurity. He has also been involved in various teaching activities in these areas.

Phillippe Van Linthout

Mr. Van Linthout is currently Judge in the Court of First Instance of Antwerp in Belgium. As an Investigating Judge, he works on a daily base in Internet and Information Security-related cases. He was appointed to treat terrorism cases as a specialised Investigating Judge (since December 2009).

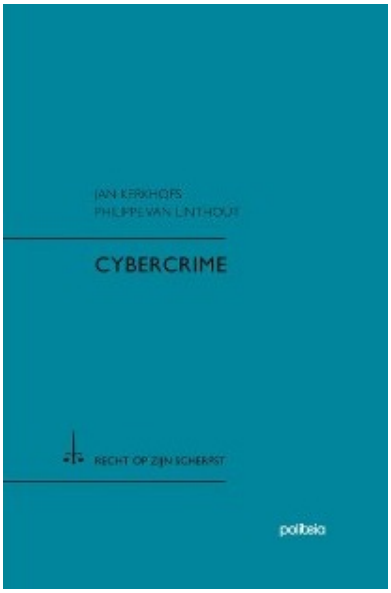
Mr. Van Linthout specialises in ICT crime and trains his fellow magistrates in the area. His career has seen him assuming various responsibilities as an Investigating Judge (since September 2006), former Deputy Public Prosecutor, Public Prosecutors Office of Dendermonde (Belgium) (Special Criminal Law Section (1998-2006)), and a Lawyer (barrister, bar of Gent - Belgium).

Mr. Van Linthout is assigned as expert of the Belgian delegation in the Convention Committee on Cybercrime (T-CY) of the Council of Europe.

Mr. Van Linthout holds the "European Certificate on Cybercrime and Electronic Evidence", École Nationale de la Magistrature (Paris - France) - CYBEX (2009), in addition to the Diploma "D.E.A. de Droit Pénal et Sciences Pénales", Université Paris II, Panthéon-Assas, France (1996) (specialisation in criminal law) and a Master in Law from the KU Leuven, Belgium (1995).

Mr Van Linthout is a lector at the KU Leuven (the Catholic University of Leuven, Institute for Criminal Law) and is magistrate-cybercrime-expert for the B-CCENTRE (The Belgian Cybercrime Centre of Excellence for Training, Research and Education). He is a member of the Belgian Cybercrime Cell (the Belgian National Cybercrime Taskforce) and the Belgian National Platform on Telecommunication. He publishes regularly on the subject of cybercrime.

Mr. Van Linthout's teaching assignments include teaching at the European Commission Technical Assistance Information Exchange Instrument (TAIEX), at the joint regional project of the European Union and the Council of Europe on cooperation against cybercrime under the Instrument of Pre-Accession Cybercrime@IPA Regional Co-operation in Criminal Justice, at the Academy of European Law (ERA), at the European Judicial Training Network (EJTN), at The Society for the Policing of Cyberspace (POLCYB) and at the Belgian Judicial Training Institute (IGO); he also trains law enforcement agents (the Standing Police Monitoring Committee-, Federal- and Local Police agents) and lawyers (barristers).



He is - together with Jan KERKHOFS who is Federal Magistrate at the Federal Prosecutor's Office in Brussels - the author of the Belgian cybercrime standard work and field manual "Cybercrime".

http://www.politeia.be/mailing/html/polpub20131021cybercrime.html

B-CCENTRE Project objectives for the Legal research track

In the B-CCENTRE Project, Work package 3 deals with the legal aspects of cybercrime. It is devoted to fundamental and applied scientific research and the development and organisation of advanced training courses in the law discipline. The research and education activities in this Work package were drawn on the expertise built up by the academic partners over the past decades and planned to provide urgently needed in-depth knowledge on specific and advanced cybercrime issues experienced by law enforcement, both police and judiciary and other involved partners, such as e.g. ISPs, registrars, barristers.

The three main research topics defined in the project relate to:

- The purpose specification principle in the Area of Freedom, Security and Justice (L1)
- Taxonomy and legal impact of illegal conduct and content risks for minors on social network sites (SNS) (L2)
- Adaptation of the Belgian criminal law and procedures to specificities of the cybercontext (L3)

Furthermore, a series of advanced legal cybercrime training modules were planned in English/Dutch (L4) and French (L5). Expert seminars were foreseen to deal with:

- Special (intrusive) investigative methods and the specificity of the cybercontext (L6)
- International legal cooperation in cybercrime matters (L7)
- Adapting Belgian criminal law and procedure to specificities of the cybercontext (L8)

The objectives set have largely been met since also additional study work has been performed by the dedicated research teams, including also researchers funded on other than B-CCENTRE resources.

Activities have resulted in a Legal Research Report (this publication), several published articles, legal education and training modules and have been presented at different conferences, seminars and training sessions. Most information on these activities is available on the B-CCENTRE website – www.b-ccentre.be.

B-CCENTRE defined Research (L1 to L3)

In the framework of the B-CCENTRE project, three specific research activities have been foreseen. The three main research topics defined in the project relate to:

- L1: the purpose specification principle in the Area of Freedom, Security and Justice
- L2: Taxonomy and legal impact of illegal conduct and content risks for minors on social network sites (SNS)
- L3: adaptation of the Belgian criminal law and procedures to specificities of the cybercontext

Hereafter a summary is provided on the research results obtained to date.

The purpose specification principle in the Area of Freedom, Security and Justice

Under L1 Fanny Coudert conducted research on the challenges faced by law enforcement authorities and the regulators to implement the purpose specification principle to regulate surveillance practices. The research resulted in the publication and presentation at internatinoal conferences of three papers that respectively dealt with the rationale of the purpose specification principle and the challenges faced in the re-use of information by law enforcement authorities, the conditions for use of this information as valid evidence before a court and finally the role that the principle of accountability can play to ensure the legitimacy of surveillance practices:

(1) Coudert, Fanny, Dumortier, Jos, Verbruggen, Frank (2012), Applying the purpose specification principle in the age of Big Data: the example of integrated video surveillance platforms in France, ICRI Research paper 6/2012. This paper explored the rationale of the purpose specification principles and the difficulties in applying this principle in the context of access by law enforcement authorities to private video recording. It dealt with the issue of the re-use of information collected by private actors for legitimate reasons for the prevention and investigation of criminal offenses.

(2) Coudert, Fanny, Gemo, Monica, Beslay, Laurent, Andritsos, Fivos (2012) Pervasive Monitoring: Appreciating Surveillance Data as Evidence in Legal Proceeding, 4th International Conference on Imaging for Crime Detection and Prevention (ICDP 2011), vol, 1-6. This paper dealt with the issue of the legitimacy of digital evidence, more specifically it analysed the conditions information collected of shared with law enforcement authorities could be used as valid evidence before courts. It looked at the specific issue of participative policing, i.e. when citizens voluntarily record events with their smartphones and share this information with the police for the investigation of criminal offenses.

(3) Coudert, Fanny (2014) Accountable Surveillance Practices: Is the EU Moving in the Right Direction?, in Lecture Notes in Computer Science, Privacy technologies and Privacy, vol 8450 2014, 70-85. Aware that the purpose specification principle cannot always act as strong a priori safeguards, this paper examined the role that can be played by the principle of accountability to ensure the legitimacy of law enforcement practices in the prevention, detection and investigation of crimes.

Taxonomy and legal impact of illegal conduct and content risks for minors on SNS

Within the framework of the B-CCENTRE project, under L2, in combination with an FWO Postdoctoral Project on Risk-reducing regulatory strategies for illegal and harmful conduct and content in online social network sites, a taxonomy of illegal and harmful content and conduct risks was developed, starting from relevant social science research (a.o. the EU Kids Online Study). Risks such as grooming, sexting and

bullying were defined, their prevalence was examined and their impact in the social network sites (SNS) environment was studied. In a second step, the applicability of the current legal framework (criminal law, privacy legislation, media regulation, fundamental rights, etc.), both at European and national (Belgian) level, to these risks was assessed.

Focusing on two risks that are particularly important in social networks, sexting[1] and cyberbullying[2], the degree of protection that this framework offers as well as the gaps in the current legislation were identified. With regard to sexting, it was found that whereas a strict interpretation of child pornography legislation could lead to its applicability to sexting, the more recent legislative documents at European level clarify that the rationale of this type of legislation is not to criminalise consensual sexual conduct between minors that have reached the age of sexual consent. Both the Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (2007) and the EU Directive on combating the sexual abuse and sexual exploitation of children and child pornography (2011) state that signatories or Member States may exclude the production and possession of sexual images by and of minors that have reached this age from criminalisation. Distribution or transmission of such images, however, may still be criminalised. Although the further transmission of sexting images (so-called 'secondary sexting') may certainly cause harm, the question remains whether this type of 'offense' should be dealt with on the basis of the provisions that were created to fight child pornography and child abuse. A new, carefully tailored legal provision to address this may be more appropriate. A relevant consideration is whether this should be a criminal provision or not. In any case, if harm does occur, it may be possible to rely on national provisions related to civil liability. Two additional concerns regarding sexting were identified. First, difficulties may arise when the age of sexual consent and the age used in provisions that are applied to sexting diverge. This can lead to situations where minors can legally engage in sexual conduct but may not take pictures that are sexually suggestive. Although from certain perspectives this may be desirable since harm may be caused if the images are used involuntarily at a later date, one may wonder whether every type of conduct that can potentially lead to harm should be regulated. At the very least, this situation may be confusing to teenagers, who may not be aware of this divergence. Second, on the basis of the image itself it may be very difficult to assess whether the image was taken voluntarily or not, as consensual sexting images may look exactly the same as images that are taken under duress. It will thus be very important to judge each case on an individual basis, taking into account the intention of the minors involved and the particular circumstances. With regard to bullying, research showed that a number of existing legislative provisions may be relevant to cases of cyberbullying on SNS. In Belgium, for instance, most of these provisions, such as provisions related to libel, defamation, harassment or stalking, are formulated in a technology-neutral manner, which implies that they may also be applied in a SNS environment. There is thus no need for new legislation to address this issue. However, this does not mean that the application of these provisions may not be confronted with obstacles, such as the potential anonymity of perpetrators or the fact that the majority of popular SNS providers are located abroad, hindering effective enforcement of the national legislative provisions.

Research results related to this topic have been presented at the International COST Cyberbullying Conference in Paris in June 2012 and the ITS Regional European Conference in Vienna in July 2012. In addition these results have been included in peer-reviewed book chapters:

- Lievens, Eva & Valcke, Peggy, "Regulatory trends in a social media context", 557-580, in: Price, Monroe & Verhulst, Stefaan, Routledge Handbook of Media Law, Routledge, 2012, 616 p.;

[1] "*Sexually explicit content communicated via text messages, smart phones, or visual and web 2.0. activities such as social networking sites*": Ringrose et al. (2012), A qualitative study of children, young people and 'sexting' - A report prepared for the NSPCC, http://www.nspcc.org.uk/Inform/resourcesforprofessionals/sexualabuse/sexting-research-report_wdf89269.pdf, 9.

[2] "*Being cruel to others by sending or posting harmful material or engaging in other forms of social cruelty using the Internet or other digital technologies*": Willard (2007), Educator's guide to cyberbullying and cyberthreats, http://csriu.org/cyberbully/docs/cbcteducator.pdf, 1.

- Lievens, Eva, "Children and peer-to-peer risks in social networks: regulating, empowering or a little bit of both?", in: van der Hof, Simone, van den Berg, Bibi, Schermer, Bart (eds), Minding Minors Wandering the Web: Regulating Online Child Safety, Information Technology & Law Series, Springer Press / Asser Press, 2014, 191-209
- Lievens, Eva, "Risico's voor jongeren op sociale netwerken bekeken vanuit juridisch perspectief", in: Valcke, Peggy, Lievens, Eva and Valgaeren, Pieter Jan (eds), Sociale Media: Actuele juridische aspecten, Intersentia, 2013, 29-66)

and peer-reviewed journal articles:

- Lievens, Eva, "Risk-reducing regulatory strategies for protecting minors in social networks", Info - The journal of policy, regulation and strategy for telecommunications, information and media 2011, Vol. 13, No. 6, 43-54
- Lievens, Eva, "Bullying and sexting in social networks: Protecting minors from criminal acts or empowering minors to cope with risky behaviour?", International Journal Crime, Law & Justice 2014, Vol. 42, Iss. 3, 251-270.

Adaptation of the Belgian criminal law and procedures to specificities of the cybercontext

Under L3 Kristel De Schepper conducts research on the adaptation of Belgian criminal law to the specificities of the cybercontext. Within this framework, she prepares a PhD entitled "Criminalisation of espionage and information abuse to protect business secrets" under the supervision of Prof. dr. Frank Verbruggen. In general, she examines whether Belgian substantive criminal law is up to the challenges of the information society.

In an information society a different approach towards the protection of valuable economic information can be considered. Management and corporate policy decisions nowadays are taken in the 'virtual world', and economically valuable information is increasingly stored on digital data systems, what makes it more vulnerable. Confidential information can be very valuable and as such, worth protecting against espionage by insiders or outside competitors. Not all information is however worth protecting because of its intrinsic value. Existing cybercrime offences often seem to focus on the *means used* to access the data, rather than on their actual *content*. This leads to a very broad *indirect* protection of *all* the digitally stored information, regardless of their intrinsic value. The criminalisation of cybercrime is therefore often a two-edged sword and the legislator needs to carefully consider possible side-effects of an extensive criminalisation. The research hypothesis is that a better focus on and a sharper definition of the legal interest (*Rechtsgut*) protected by specific offences, will lead to more respect for the idea of criminal law as the ultimate resort and to a more efficient use of criminal law. On the basis of a case study of economic espionage and the violation of business secrets, the research intends to establish the criteria which should guide lawmakers considering the creation and use of criminal law.

The PhD is expected to be defended at the KU Leuven in 2017. Preliminary research was presented at a conference organised by the Centre for Methodology of Law at the KU Leuven on May 12, 2011, initial results at a seminar "Cyber Space Invaders: Criminal Jurisdiction on the Internet" organised by the B-CCENTRE and the Leuven Centre for Global Governance Studies on October 2, 2012 in Leuven and at a doctoral seminar "'Data espionage': traditional property offences versus IT-specific offences. On the difficulties to define legal goods in a digitised society" at the Institute of Criminal Law on June 21, 2013. The first presentation resulted in a substantive contribution in the book "Zakengeheim" (*Trade secrets*), published in 2012. Other topics related to the research were also disseminated in peer-reviewed journals *Auteurs & Media* in 2012 and *Tijdschrift voor Strafrecht* in 2013. These articles focus on jurisdictional issues in a cybercontext and more specific on the Belgian Yahoo case. A judicial saga started when the Belgian prosecution service sued US dotcom Yahoo, Inc in a Belgian criminal court for its failure to respond to a Belgian prosecutor's request to reveal data concerning Belgian Yahoo-clients. This case illustrates as no

other the problems of jurisdiction in a digital context. When the Belgian criminal law enforcement power to order data-handover is applied to a non-resident foreign ICT-operator and the failure to comply amounts to a Belgian criminal offence, the jurisdiction issues become very complex. These issues, and more specific the location problems in cyber investigation and the enforceability of the duty to cooperate of ISPs, appear to be a crucial challenge in the area of cybercrime and will most likely be the subject of further fundamental academic research the upcoming years.

Publications - Abstracts

Guidelines For Privacy-Friendly Default Settings

Ausloos, J., Kindt, E., Lievens, E., Valcke, P., & Dumortier, J.

The debates regarding privacy on social networks often relate to the amount of control an individual has - or should have - over his/her personal data. This has resulted in many social networks gearing up their privacy settings panes, offering more fine-grained control to their users. Paradoxically, it seems as if these controls do not contribute (a lot) to the protection of individuals' privacy in practice. Every control in the privacy settings pane has a 'default', a value to which it is set when the user remains inactive. Naturally, most social networks align these default settings to their own business interests which usually do not coincide with their users' privacy interests. This paper attempts to evaluate the importance of having in place 'privacy-friendly default settings' as a way to protect individuals' privacy and personal data more effectively. After a critical assessment of their benefits and drawbacks, the paper sets forth some concrete guidelines that can be used to establish privacy-friendly (default) settings. Last, but not least, the paper evaluates the potential legal bases of such privacy-friendly default settings.

Ausloos, J., Kindt, E., Lievens, E., Valcke, P., & Dumortier, J. (2013). Guidelines For Privacy-Friendly Default Settings. ICRI Working Paper Series.

Les perspectives de légitimation des échanges des oeuvres sur les réseaux peer-to-peer en Belgique

Colin, C. and Dusollier, S.

Les échanges illégaux d'oeuvres sur les réseaux peer-to-peer sont un phénomène difficile à combattre. Si une solution répressive de type HADOPI constitue l'une des voies possibles, elle n'est pas la seule. Il pourrait être envisageable d'élaborer un système d'autorisation de ces échanges tout en rémunérant les titulaires de droits pour l'exploitation ainsi faite de leurs oeuvres. Telle est l'orientation — dans les grandes lignes et en gardant à l'esprit leur différence de philosophie — des deux propositions de lois belges récentes appréhendant cette problématique. Ce dispositif d'autorisation se fonderait nécessairement sur un contrat impliquant les fournisseurs d'accès à Internet et les titulaires de droits à travers les sociétés de gestion collective. Plusieurs variantes de contrats sont possibles, dépendant du degré d'implication des fournisseurs d'accès dans le modèle. Et tout l'enjeu est là : comment réussir à convaincre les fournisseurs d'accès à Internet de jouer un rôle dans ce dispositif alors qu'a priori rien ne les y incite ? L'article propose une réflexion sur le modèle contractuel pouvant être mis en place pour autoriser les échanges en peer-to-peer ainsi que sur les moyens pouvant amener les fournisseurs d'accès à s'impliquer dans de tels processus contractuels.

Colin, C. and Dusollier, S. (2012). Les perspectives de légitimation des échanges des oeuvres sur les réseaux peer-to-peer en Belgique. Larcier, 259-305.

Locating criminal investigative measures in a virtual environment. Where do searches take place in cyberspace?

Conings, C.

State sovereignty is aimed at the organisation of a society and the protection of its citizens and their fundamental rights. Its existence depends upon internal recognition (by the people subjected to the sovereign power) and external recognition (by other sovereign states). In order to fulfil its organising and protective function, a state enjoys a range of powers, such as the power to prescribe and adjudicate

behaviour and the power to enforce law. Those powers are basically limited to a specified *territory*. The restricted territorial scope enables the peaceful coexistence of equal sovereign states, which are similarly responsible for order and peace within their territory. However, it is not always clear where to draw the territorial line. Within its territory, a state is empowered to prohibit certain acts through criminal law. Nevertheless, sometimes the localisation of the criminal behaviour seems difficult. Therefore, legal doctrine spelled out multiple localisation theories which help determine the *locus commissi delicti,* for example by means of the activity criterion or the ubiquity criterion. The same problem occurs in the context of criminal procedure, more specifically the criminal investigation phase. The problem arises whenever the location of the evidence sought is not clear or the location of access to the evidence differs from the location of the evidence itself. Where does a wiretap take place? Where do we have to locate a visual surveillance? Which location is decisive: the location of the subject under investigation, the location of the evidence searched for or the location of the investigating authority? Although the localisation difficulty clearly arose with regard to these more traditional investigation measures, the problem was never explicitly addressed. With respect to interception of telecommunications, the EU convention on mutual assistance in criminal matters however silently shifts focus in localising the investigative action from the object sought to the subject under investigation. Today, we can no longer put off dealing with this problem in a more explicit manner. The digitalisation of evidence confronts us more than ever with these questions. Where do digital (remote) searches take place? The current European nor international framework provides us with a clear answer. After going through the different existing approaches of the European Union and Council of Europe, we take a step back and try to answer the localisation question by referring to the *ratio* of territorial sovereignty. The following questions are therefore at the heart of the paper: Where should we locate (digital) investigation measures in order to maintain the desired interplay between fundamental rights protection, sovereignty and territoriality? What position should the EU and Council of Europe adopt in this matter in order to restore the balance between (1) internal power to organise society and protect fundamental rights (including the power to exclude other states) and (2) the need for external cooperation and bonding? Which approach can assure the full effect of the Rule of Law within a virtual context?

Conings, C. (2013). Locating criminal investigative measures in a virtual environment. Where do searches take place in cyberspace?. NC (dutch) & see Annex I of this B-CCENTRE Legal Research Report (English)

Traditional forgery vs. IT forgery (in Dutch: Reële Valsheid Vs Virtuele Valsheid.).

Conings, C.

The computer crime act of 28 November 2000 provided a first "update" of the Belgian criminal law and procedure law, driven by ICT developments and their potential abuse. IT forgery got introduced into the Belgian Criminal Code as a new offence, turning the creation and use of false digital files into an offence. This offence however shows striking similarities to the traditional crime of forgery. The question is therefore which characteristics distinguish one offence from the other. Do these characteristics justify the different legal regimes for each one of them?

A comparison of both criminal acts clarifies that the difference lies exclusively in the object thereof. The traditional crime of forgery concerns the falsification of non-computerised, written data. In contrast, the IT forgery refers to computer data, which includes visual and spoken representations of information. In practice, it is often difficult to make the distinction. Moreover, the use of different criminal provisions leads to different treatment of similar situations. The result of legislative intervention is therefore incompatible with the "offline=online" principle which the legislator had established at the outset.

A fusion of both into one offence with a larger object seems appropriate. The legislator acknowledged the problem of the outdated and complex Belgian legal framework concerning forgery in 2000. It is time to solve this problem by creating a new, single and simplified offence of "forgery of legally relevant information".

Conings, C. (2013). Reële Valsheid Vs Virtuele Valsheid. NjW.

Remote searches: borderless or pushing back frontiers? (in Dutch: Van een netwerkzoeking naar online doorzoeking: grenzeloos of grensverleggend?)

Conings, C., & Oerlemans, J.J.

A network search allows law enforcement officers to investigate IT systems remotely. The exact scope of the investigative measure is not always clear though. In the article, the authors examine whether the investigative measure can only be applied starting from an IT-system already under investigation or whether it also allows law enforcement to investigate systems remotely, starting from their own IT systems. Furthermore, the authors look into the (im)possiblity to apply the power covertly. They finish by looking into the jurisdictional issues, related to remote searches of computer systems. Throughout the article, the authors look at the Belgian as well as the Dutch approach, which reveals interesting similarities and differences between both legal frameworks.

Conings, C., & Oerlemans, J.J. (2013). Van een netwerkzoeking naar online doorzoeking. Computerrecht

Social media: a new challenge for law enforcement. (in Dutch: Sociale media Een nieuwe uitdaging voor politie en justitie

Conings, C., & Van Linthout, P.

Over the last decade, several technical evolutions made it possible for each one of us to participate actively in the creation of a new phenomenon often called the web 2.0. With the emergence of different forms of social media people can create webpages without any help of computer experts and easily share all sorts of information through different types of platforms. They can sell or buy goods on the internet, communicate by chat, by video or by voice, share their latest holiday photos or even their deepest thoughts. However, the possibilities that cyberspace has to offer are not only beneficial to well-intended people but also to diverse types of (cyber)criminals. Not only can crime be committed in this new, virtual world. Social media are also an important tool to help criminals in committing their crimes in real world or to facilitate the communication and organisation of criminal groups. That is why social media enclose a load of information which can be precious for law enforcement. This contribution looks at the different legal possibilities and problems which law enforcement can face while taking access to social media, while investigating within these social media and when 'social-media-evidence' is used in court. Due to the fact that Belgian criminal procedural law still focuses on the real world, law enforcement faces plenty of legal difficulties and legislative action is long overdue. Nevertheless this text makes clear that a creative and open-minded approach of the matter can already offer important opportunities in investigating crime. In other words, law enforcement can also enjoy the possibilities of social media, even today, but these possibilities are only a small part of the bigger picture, which requires legislative intervention.

Conings, C., & Van Linthout, P. (2012). Sociale media Een nieuwe uitdaging voor politie en justitie. Panopticon.

Privacy and the regulation of 2012

Costa, L. and Poullet, Y.

This paper explores the European Commission's proposal for a new Regulation to update and reform data protection law in Europe. As regards the Regulation itself, without presenting an exhaustive analysis of all the provisions, this paper aims to highlight some significant changes proposed to the data protection regime by comparison between Directive 95/46 and the proposed Regulation. It takes particularly into account legislative innovation concerning data protection principles, data subjects' rights, data controllers and data processors obligations, and the regulation of technologies. Before analyzing these

innovations, it introduces some considerations about the Commission's choice to use a Regulation instead of a Directive to harmonise national data protection regime.

Costa, L. and Poullet, Y. (2012). Privacy and the regulation of 2012. C.L.S.R., 254-262.

Applying the purpose specification principle in the age of "Big Data": the example of integrated video surveillance platforms in France

Coudert, F., Dumortier, J., & Verbruggen, F.

The proliferation of data made available to businesses, governments and individuals, also referred to as the "data tsunami" or the age of "big data", heavily challenges the application in practice of the purpose specification principle, one cornerstone principle of the data protection framework. In order to illustrate these difficulties, this paper takes as example a growing phenomenon, the deployment of integrated video surveillance platforms that link networks originally installed for distinct purposes and managed by different actors. Focus is put on France where the government passed a law to authorise law enforcement agencies to access private video surveillance networks for purposes of fighting crimes against properties and persons. We conclude by formulating policy recommendations tending to counter the dilution of safeguards when implementing the purpose specification principle in networked systems.

Coudert, F., Dumortier, J., & Verbruggen, F. (2012). Applying the purpose specification principle in the age of "Big Data": the example of integrated video surveillance platforms in France. ICRI Working Paper Series.

Accountable Surveillance Practices: Is the EU Moving in the Right Direction?

Coudert, F.

The European Union is introducing into the Data Protection Package a new data protection principle, the principle of accountability. Data controllers will be compelled to adopt policies, organisational and technical measures to ensure and be able to demonstrate compliance with the legal framework. The expected benefits are threefold: to foster trust in personal data management practices of data controllers, to increase visibility of personal data processing activities and to raise data controllers' privacy awareness. Surveillance practices, because of their inherent opacity, could greatly benefit from reinforced accountability obligations to gain public's trust. This paper critically analyses whether the policy options taken by the European Union to operationalise the principle of accountability are likely to meet this goal.

Coudert, Fanny (2014) Accountable Surveillance Practices: Is the EU Moving in the Right Direction?, in Lecture Notes in Computer Science, Privacy technologies and Privacy, vol 8450 2014, 70-85

Pervasive Monitoring: Appreciating Citizen's Surveillance as Digital Evidence in Legal Proceedings

Coudert, F., Gemo, M., Beslay, L., & Andritsos, F.

Images or video streams, extracted from data acquired through surveillance systems and intended to be used as evidence in court, should have all attributes of conventional digital evidence, meaning that they should be admissible, authentic, reliable, complete and believable. This paper discusses the first three attributes that surveillance systems should comply with to be submitted as evidence in legal proceedings and it identifies some of the obstacles in the way through harmonisation. The focus is on data gathered from a range of ad hoc sources present at the scene of an incident, including smartphones and wireless sensor networks (used for safety, security or traffic management/environmental monitoring). New

scenarios for crowd-sourced surveillance mediated by law enforcement supervision are further considered. Specific attention is brought to the compliance with privacy requirements that often condition the admissibility of the evidence.

Coudert, F., Gemo, M., Beslay, L., & Andritsos, F. (2011). Pervasive Monitoring: Appreciating Citizen's Surveillance as Digital Evidence in Legal Proceedings. 4th International Conference on Imaging for Crime Detection and Prevention (ICDP 2011).

Le droit au respect de la vie privée face aux nouvelles technologies

Degrave, E. and Poullet, Y.

Souligner l'impact de l'article 22 de la Constitution sur le développement des technologies fait écho aux commentaires divers entendus sur les bancs du Sénat lors des travaux de la révision constitutionnelle de 1994 qui introduisit l'article 22 dans la Charte fondamentale de la Belgique. La Constitution se doit de traduire les « principes essentiels qui doivent gouverner sa société», « être le reflet de conscience de son peuple et des exigences qu'il attend du pouvoir » et donc « traduire fidèlement l'évolution de sa pensée (...). Dès lors, il apparaît essentiel que la vie privée et familiale soit protégée des risques d'ingérence que peuvent constituer, notamment par le biais de la modernisation constante des techniques de l'information, les mesures d'investigation, d'enquête et de contrôle menées par les pouvoirs publics et organismes privées ». En d'autres termes, la considération des risques encourus par nos libertés du fait des technologies nouvelles était d'emblée au cœur des préoccupations de nos constituants lorsqu'il s'est agi de justifier la consécration de l'article 22 de la Constitution.

Degrave, E. and Poullet, Y. (2011). Le droit au respect de la vie privée face aux nouvelles technologies. Les droits constitutionnels en Belgique, 1001-1035.

Removing and Blocking Illegal Online Content

Demeyer, K., Lievens, E., & Dumortier, J.

In 2011, the Directive of the European Parliament and of the Council on Combating the Sexual Abuse, Sexual Exploitation of Children and Child Pornography was adopted, repealing and updating the 2004 Framework Decision on this topic. The much debated Article 25 of this proposal requires Member States to ensure the prompt removal of child pornography websites hosted in their territory and to endeavor to obtain the removal of such websites hosted outside their territory. It also leaves the option for Member States, subject to several safeguards, to block access to such websites to users within their territory. Both these policy choices are highly controversial and much debated, both at the level of the European Union and within Member States. This article analyzes both mechanisms, describing them from a technical as well as a legal point of view, in order to provide more clarity as to the advantages and drawbacks of these policy options.

Demeyer, K., Lievens, E., & Dumortier, J. (2012). Removing And Blocking Illegal Online Content. Policy & Internet. doi: 10.1002/poi3.8.

The protection of business secrets in criminal law: 'send in the cavalry'?

De Schepper, K. & Verbruggen, F.

In recent years, the press continuously reported about companies that were experiencing problems with economic espionage and the "loss" of sensitive information. How should we deal with such modern threats? Our Belgian Criminal Code and Criminal Procedure Code, after all, still date back to the time of the horse and carriage: the nineteenth century. Hence the almost sacred importance attached to

writings, hence the heavy penalties in the Penal Code for property crimes. That nineteenth century also saw the last heyday of the cavalry: as army unit mobile, overwhelming and difficult to stop, but sometimes also proud and increasingly vulnerable due to the development of new weaponry. The judicious use of the cavalry made it possible to recover from seemingly lost situations and often decided crucial battles. Criminal law is actually the cavalry of law, the little discrete forces that were called upon in need.

Is such nineteenth-century legal heavy cavalry still appropriate in the twenty-first century information society? In that society the evident value of physical, tangible and removable goods is less outspoken compared to that of intangible assets and "information" is an important but difficult definable legal interest. One should however not be a card player to know that it is much more difficult, or less interesting, to play either with all cards on the table or with a "snitch" who briefs your adversary. Consequently, is seems to be obvious that secret information as a socially valuable legal interest deserves protection under criminal law. Yet this complex legal matter has largely remained criminal wasteland. We hope to change that in the future, but it explains why this contribution only purports to be a timid and incomplete exploration and why it is limited to pointing out some substantive criminal law opportunities and challenges for the criminal procedure in this context.

De Schepper, K. en Verbruggen, F. (2012), De bescherming van het zakengeheim in het strafrecht: cavalerie of calvarie? In Zakengeheim, die Keure, 131-188.

How to enforce a duty to cooperate in a virtual context?

De Schepper, K.

On October 12, 2012, the court of appeals of Brussels discharged US-based company Yahoo! Inc. of the Belgian omission offence of a refusal to cooperate with the Belgian legal authorities. This article comments on this judgment. According to the author, the duty to cooperate of article 46bis of the (Belgian) Criminal Procedure Code also applies to foreign providers of electronic communication services when they actively offer these services in Belgium. The location of the establishment is therefore not decisive for the territorial scope of the Belgian criminal offence of a refusal to cooperate. It however does determine the way in which the public prosecutor can activate this procedural duty to cooperate. That should happen by relying on legal assistance from US authorities. The 'virtual accessibility' of these entities does not detach Belgium of its international obligations to use formal channels of communication.

De Schepper, K. (2012). Medewerking in een virtuele context? Ya! Hoo echter afdwingen?, A&M, 239-243.

Belgian substantive and formal criminal jurisdiction in the case of prosecution of foreign electronic service providers for failure to cooperate. Can Alien Space Invaders evade the Belgian Pac-Man?

De Schepper, K & Verbruggen, F.

The Belgian Yahoo case revolves around the territorial scope of a duty to cooperate with a criminal investigation, particularly in the case of IT-service-providers without physical presence on the Belgian territory. Article 46bis of the Belgian Code of Criminal Procedure imposes a duty to identify an ICT-application or its user, when ordered to by a Belgian public prosecutor. Belgian law enforces this duty by imposing a criminal fine in case of refusal or insufficient co-operation. The Yahoo-case raised the question how Belgium could enforce this investigative measure and use the criminal sanction in a trans-border IT context and the question whether foreign electronic service providers can be punished by the Belgian criminal courts for ignoring a direct order from a Belgian prosecutor?

The vast possibilities which electronic communications offer to the public, create a corollary need for investigators rapidly to obtain access to such information. As Belgium uses criminal punishment to ensure

the co-operation of private entities with investigative measures, the case illustrates the intricate interrelation of substantive criminal law jurisdiction (punishment of certain acts) with procedural criminal law jurisdiction claims (the legal obligation to cooperate with a criminal investigation). This interrelation complicates the answer to the classical question which State can claim jurisdiction over the internet, its players and its users. International public law regulates and limits the jurisdictional claims of individual States, Traditionally, it has appeared less opposed to an extensive application of substantive criminal law by States ("substantive criminal jurisdiction claims"), as long as those states do not effectively press home these claims through the trans-border use of force or compulsion, of intrusive law enforcement actions or the imposition of sanctions. This "procedural criminal jurisdiction" is therefore more likely to enter into conflict with the territorial sovereignty of other states. Do the traditional criteria of international law, which originate from the real world of physical national borders, still apply in the "virtual world" of the internet?

Belgium's broad substantive criminal jurisdiction over those who fail to co-operate with Belgian law enforcement does not present an international legal problem, but the authors believe Belgium cannot use this offence to obtain foreign evidence from foreign-based operators without respecting the international rules on mutual assistance in criminal matters. They reject the extensive interpretation of Belgian territorial jurisdiction invoked by the Belgian prosecutor. That broad substantive territorial scope of substantive criminal law should not, in their view, be used to circumvent international law limits on extraterritorial law enforcement activity. That being said, the case illustrates all the more clearly how pressing the need for more workable international cooperation is in the digital context. States should reach agreements which provide law enforcement from partner countries easy access to certain data.

De Schepper, K. & Verbruggen, F. (2013). Ontsnappen Space Invaders aan onze pacmannen? De materiële en formele strafrechtsmacht van België bij strafbare weigering van medewerking door elektronische diensverleners, T. Strafr., 143-166 (Dutch) & English version in this B-CCENTRE Legal Research Report

The 'cloudy' limits of IT-forgery and IT-fraud

De Schepper, K.

This article annotates a recent decision in an interesting cybercrime case. This decision allows us to analyse some tricky legal issues related to IT-forgery and IT-fraud, like the different criminal protection of forged writings and forged data, the interpretation of the constitutive element 'legal value' of IT-forgery and the very broad criminalisation of IT-fraud.

De Schepper, K. (2015), De troebele grenzen van informaticavalsheid en informaticabedrog, (upcoming)

Criminal law in the business practice

De Schepper, K. and many others

This book approaches criminal law and criminal procedure from the practical standpoint of the business practitioner. The criminal law as a business risk is for many business practitioners still very unknown. However the actuality indicates that the criminal risks to the business are not negligible. Criminal law deserves more attention in the risk management of most enterprises. Its risk should be thoroughly assessed and analyzed. This allows the business practitioner to formulate an appropriate policy to deal with these risks (criminal liability, fraud, criminal investigations, etc.). Hence, this book is primarily addressed to managers, risk managers, corporate lawyers, internal and external audit services, etc., who wish to overcome the "criminal" vulnerability of their company. The book also pays attention to cybercrime, which is a growing problem in the context of the business practice, and to cyber investigation, given the emerging importance of these investigative measures and duties to cooperate with law enforcement in that context.

Strafrecht in de onderneming – derde herziene editie, Intersentia, to be published in 2015

La surveillance par caméras: de la supervision de lieux vers l'observation systématique de personnes

Dumortier, F.

La délimitation entre le champ d'application de la loi caméras et celui de l'article 47sexies du Code d'instruction criminelle est encore devenue plus incertaine à la suite de l'évolution technologique récente des caméras. Outre le fait que celles-ci sont souvent utilisées en réseau et connectées à des bases de données, elles peuvent actuellement être couplées à des algorithmes qui leur permettent aisément de « suivre » une personne déterminée ou de repérer automatiquement des évènements et objets particuliers dans des lieurs relativement vastes. En l'état actuel de la législation, une telle observation proactive systématique de personnes par ces acteurs privés peut-elle être qualifiée de traitement de données judiciaires illicite au sens de l'article 8 de la loi vie privée si elle n'est pas réalisées sous le contrôle d'une autorité publique dans le conditions fixées par l'article 47sexies du Code d'instruction criminelle ?

Dumortier, F. (2013). La surveillance par caméras: de la supervision de lieux vers l'observation systématique de personnes. Anthemis, 333-342.

Europe's Fragmented Approach Towards Cyber Security

E Silva, K.

The article proposes a deeper insight into the variety of concepts used to describe the term cyber security and the ways in which it has been used in recent years. It examines the role of three important actors involved in the internet governance arena, namely governments, private sector and civil society, and how they have influenced the debate. To this end, this paper analyses how different organisations, industry and societal actors see cyber security and how their interests influence the way the debate has evolved. The difficult balance between security and fundamental rights, although not new to governments and society, is of great importance for the internet. Citizens have engaged in favour of an open internet. However, little attention has been paid to the demands of citizens and how they may contribute to a concept of cyber security that brings society to its core. The paper states that for cyberspace to be open and supportive of innovation, the practice of cyber security needs to internalise the interests and perspectives of end users. A multistakeholder approach to cyber security asks a more participative environment where the rules of the game are decided with public participation and consultation, giving citizens the means and methods to influence the way cyber security is conceived and implemented. The paper concludes that although a citizen centric approach towards cyber security should be the way forward, this seems to be yet far from being included in the governmental agenda. The methodology applied in the paper was mainly focused on desk research.

E Silva, K. (2013). Europe's Fragmented Approach Towards Cyber Security. Internet Policy Review. doi: 10.14763/2013.4.202.

EU Information Sharing Platforms: Cybercrime Meets Data Protection

E Silva, K.

Recently, information sharing initiatives focused on the fight against cyber crime have become more and more popular. The proliferation of these platforms can be associated to the need for cooperative efforts from different stakeholders, as well as to the private sector control of the IT operations in the market. IT companies have risen to be strategic players in promoting and ensuring security. Effective information sharing calls for distribution of key information that often classifies as personal data in the terms of the law. Despite the proliferation of information exchange against cyber crime, this process was not followed by a more flexible application of data protection rules. This has created a grey zone in which security experts may be violating the fundamental right to privacy and data protection while trying to keep Internet safe. The goal of this paper is to clarify the data protection mechanism applicable to the activities of many technicians, who are often far from legal discussions and do not understand the legal issues involved in their work. It aims to bridge the gap between lawyers and security experts while providing short guidance on how to take part in information sharing systems without violating data protection laws. Finally, it aims to fortify the response against cyber crime by incentivising stakeholders to join efforts in cooperative networks within the limits of the law.

E Silva. K. (2014). EU Information Sharing Platforms: Cybercrime Meets Data Protection. Future Security 2014, Sep 2014, Conference Proceedings (upcoming).

Zombie Alert: Assessing Legitimacy of P2P Botnet Mitigation Techniques

E Silva, K. & Roex, R.

This paper covers the legal analysis of crawling, a technically relatively advanced technique for gathering intelligence on a P2P botnet, a decentralised network of infected computers under the control of a bot master. The intel acquired via the crawling technique can subsequently be used to deploy mitigation techniques such as sinkholing, which disrupts botnet operations. We have chosen crawling for its relevance in practice as well as the attention it has been given in scholarly discourse. In the article, we present a high level overview of the technique's basic functionalities and requirements, before we perform a legal assessment of the legitimacy of the different aspect of this technique according to data protection and criminal procedure law. In this paper, we look at crawling as a technique against P2P botnets to examine two questions: 1. What are the legal grounds justifying the use of crawling by private sector and individuals, with special attention to data protection legislation; 2. What are the legal grounds justifying the use of crawling by law enforcement and their value in court. Due to our familiarity with the Belgian and Dutch legal systems, the analysis of the aforementioned questions is limited to the legal frameworks of Belgium and The Netherlands. Therefore, we look at the differences between both jurisdictions in dealing with the issues that arise when crawlers are used by private sector and individuals as an intelligence gathering technique and by law enforcement in a criminal investigation.

E Silva, K. and Roex, R. (2014). Zombie Alert: Assessing Legitimacy of P2P Botnet Mitigation Techniques. 25th ITS Europe, June 2014, Telecommunications Policy, Elsevier (upcoming).

How to dismantle a botnet - the legal behind the scenes

E Silva, K.

Law enforcement actions targeting botnets have recently gained greater attention. The past year struck our attention with international takeover and takedown efforts led by cooperative networks formed by industry and law enforcement. A closer look into the Gameover Zeus & Cryptolocker (2014, U.S.) disruptions reveals that law enforcement has found creative ways to investigate and prosecute

botmasters. The analysis of the Gameover Zeus & Cryptolocker disruptive operations is a powerful source of clarifications for security experts and law enforcement agents. Today several questions left unanswered could pave the way to the future of botnet disruptions. For instance, what made those legal actions possible, while others are still on the waitlist? What is actually stopping law enforcement from taking action; in cases they already informed on the existence and functioning of botnets? Why is the U.S. leading the botnet fight? By looking at the operations recently led by U.S. law enforcement and the takedown of Bredolab in the NL in 2010, this paper aims to answer the questions above and approximate security experts from the struggles and barriers faced by law enforcement in the EU and overseas.

E Silva, K. (2014) How to dismantle a botnet - the legal behind the scenes, conference proceedings BotConf2014 (upcoming)

Legal aspects: biometric data evidence rules and trusted identities

Kindt, E.J.

Biometric characteristics could play a role as means for binding electronic documents and transactions to a person and for identifying that person. However, one of the conditions for biometric methods to be used as an electronic signature, is that spoofing vulnerabilities are adequately assessed and appropriate solutions are developed. Anti-spoofing measures are also crucial in electronic identity schemes which may include biometric characteristics. For these schemes, privacy and data protection issues remain to be solved as well.

Kindt, E.J. (2014). Legal aspects: biometric data evidence rules and trusted identities. Handbook of Biometric Anti-Spoofing.

Privacy and Data Protection Issues of Biometric Applications: A Comparative Legal Analysis

Kindt, E.J.

Biometric characteristics, such as facial images, fingerprints, iris and voice, are increasingly used in automated systems to identify, to recognise or to verify identity claims of persons. An appropriate legal framework for biometric applications is however not yet in place. This book discusses all critical privacy and data protection aspects of biometric systems from a legal perspective. The book which has an interdisciplinary approach contains an explanation of the functioning of biometric systems in general terms for non-specialists. It continues with a description of the legal nature of biometric data and makes a comparison with DNA and biological material and the regulation thereof. It further reviews the opinions of data protection authorities in relation to biometric systems and current and future EU law, whereby a detailed analysis is made of the situation in Belgium, France and the Netherlands. It concludes with an evaluation of the proportionality principle and the application of data protection law to biometric data processing operations, mainly in the private sector, and with several suggestions for more safeguards in legislation.

Kindt, E.J. (2013). Privacy and Data Protection Issues of Biometric Applications: A Comparative Legal Analysis. Law, Governance and Technology Series.

Best Practices For Privacy And Data Protection For The Processing Of Biometric Data

Kindt, E.J.

Self-regulatory initiatives by data controllers can contribute to a better enforcement of data protection rules. This is especially important for the use of biometric data in identity management systems, because

of risks of use as unique identifiers and identification. This chapter explains the Best Practices which were developed in the Turbine project. These Best Practices recommend inter alia the creation of multiple trusted revocable protected biometric identities, which are irre- versible and unlinkable.

Kindt, E.J. (2013). Best Practices For Privacy And Data Protection For The Processing Of Biometric Data. Security and Privacy in Biometrics. doi: 10.1007/978-1-4471-5230-9.

Bullying and sexting in social networks from a legal perspective: Between enforcement and empowerment

Lievens, E.

The availability and use of social networking sites creates both opportunities and risks for their young users. This paper evaluates the applicability of the current legal framework to (cyber)bullying and sexting, two types of behaviour that are increasingly occurring between peers in the social networking environment. The analysis includes a mapping of applicable provisions at the European and national level, an analysis of the Terms of Service of two social networking providers and an overview and assessment of self-regulatory initiatives that have been taken by the industry in this area. The ultimate goal is to identify a number of elements for a comprehensive strategy to ensure that risks of (cyber)bullying and sexting are dealt with in a manner that empowers young users.

Lievens, E. (2012). Bullying and sexting in social networks from a legal perspective: Between enforcement and empowerment. ICRI Working Paper Series. Also: *LIEVENS, E. (2014), "Bullying and sexting in social networks: Protecting minors from criminal acts or empowering minors to cope with risky behaviour?", International Journal Crime, Law & Justice, Vol. 42, Iss. 3, 251-270; Lievens, E. (2013), "Risico's voor jongeren op sociale netwerken bekeken vanuit juridisch perspectief", in: Valcke, Peggy, Lievens, Eva and Valgaeren, Pieter Jan (eds), Sociale Media: Actuele juridische aspecten, Intersentia, 29-66*

Children and peer-to-peer risks in social networks: regulating, empowering or a little bit of both

Lievens, E.

Social networking services (SNS) are an important part of many children and teenager's media use. As they communicate and share content by means of these services, minors may also engage in more risky behaviour, leading to reciprocal harassment which may blur the lines between victims and offenders to a greater extent than in the offline world. However, due to the specific nature of SNS, the use, and especially the implementation and enforcement of, traditional types of legislation are confronted with many obstacles. After identifying certain legal implications, this chapter examines the potential of alternative regulatory mechanisms and empowerment techniques (co-regulation, technical tools, media literacy, information provision mechanisms). The goal is to provide guidelines for the development of regulatory strategies which reduce peer-to-peer conduct and content risks in user-centric environments for children and young people while safeguarding fundamental rights and public interest goals.

LIEVENS, E. (2014), "Children and peer-to-peer risks in social networks: regulating, empowering or a little bit of both?", in: VAN DER HOF, Simone, VAN DEN BERG, Bibi, SCHERMER, Bart (eds), Minding Minors Wandering the Web: Regulating Online Child Safety, Information Technology & Law Series, Springer Press / Asser Press, 191-209

Les saisies et perquisitions de matériel informatique : les "garde-fous" entourant leur mise en oeuvre

Losdyck, B.

Les saisies portant sur du matériel informatique peuvent avoir lieu dans bon nombre d'hypothèses : commercial, pénal, droit d'auteurs et droits voisins, ...Il appert, dans la pratique, que les saisies et perquisitions de matériel électronique sont de plus en plus fréquentes tant dans le milieu professionnel qu'ailleurs. Bien que l'on comprenne aisément le développement de ces pratiques et l'utilité de recourir à celles-ci, se pose aujourd'hui la question de savoir si celles-ci sont entourées de garanties suffisantes afin d'assurer le respect des droits de l'individu, notamment le droit au respect de sa vie privée.

Losdyck, B. (2013). Les saisies et perquisitions de matériel informatique : les "garde-fous" entourant leur mise en oeuvre. R.D.T.I., n°52, 21-49.

Chronique de jurisprudence – criminalité informatique 2009-2011

Omrani, F. and Dumortier, F.

Au cours des trois années de jurisprudence couverte par cette chronique 2009-2011, d'importantes décisions ont été prononcées en matière de hacking, de possession d'images pédopornographiques (l'affaire Hissel) mais aussi quant à la notion de fournisseur de services de communications électroniques (l'affaire Yahoo !) La présente chronique aborde successivement le faux en informatique, la fraude informatique, l'abus de confiance, le hacking, le délit de presse, le harcèlement et la possession d'image pédo-pornographique mais aussi des questions de procédures. Bien qu'il soit prématuré de faire état d'une tendance à proprement parler, on relève que les cours et tribunaux ont appliqué des infractions de droit commun à des données informatiques dans le cadre du délit de presse et de l'abus de confiance.

Omrani, F. and Dumorier, F. (2014). Chronique de jurisprudence – criminalité informatique 2009-2011. R.D.T.I., n°48-49, 198-208.

Identiteitsdiefstal via sociale media. Een juridische benadering van een maatschappelijk fenomeen

Roex, R.

Social media, to be understood as internet based applications associated with the ideological and technological foundations of the Web 2.0, have demonstrated their ability to reach a vast number of people simultaneously. Such a wide reach entails significant opportunities for economic and social exploitation. In this contribution we zoom in on the dark side of these social media and look at how criminals exploit them via a phenomenon commonly referred to as 'identity theft'. The main objective is to outline how the Belgian legal framework aims to cope with this particular type of criminal conduct. By first selecting an acceptable definition of the phenomenon and then analysing the applicable legal framework as well as recent case law, we can conclude that a) the law provides several provisions which qualify as candidates for penalising identity theft, and b) that the procedural tools foreseen in the Belgian Criminal Procedure Code through broad interpretation of the Court of Cassation allow law enforcement to take decisive action.

Roex, R. (2013). Identiteitsdiefstal via sociale media. Een juridische benadering van een maatschappelijk fenomeen. Sociale media – Actuele juridische aspecten Intersentia.

Uw data op straat: toedekken of melden? De meldplicht bij gegevenslekken: een stand van zaken

Roex, R.

Data breaches seem to be everywhere nowadays, causing damage to organisations irrespective of their size. A data breach has an impact on several different stakeholders at once, from the individual seeing his data published on the web to companies suffering civil liabilities and governments confronted with increased public expenditure to cope with the phenomenon. It is therefore important that every single one of these stakeholders takes active initiatives towards mitigating the effects of a breach, including reporting them. The contribution provides an overview of the currently applicable obligations to report and those that are in the regulatory pipeline.

Roex, R. (2014) Uw data op straat: toedekken of melden? De meldplicht bij gegevenslekken: een stand van zaken. Private Veiligheid Politeia.

Les mesures de filtrage et de blocage de contenus sur l'internet: un mal (vraiment) nécessaire dans une société démocratique ? Quelques réflexions autour de la liberté d'expression

Van Enis, Q.

Les mesures de filtrage et de blocage sont susceptibles de mettre à mal la liberté d'expression sur le réseau. La présente étude vise à analyser l'impact de telles mesures sur le droit protégé par l'article 10 de la Convention européenne des droits de l'homme. Une attention particulière est accordée à l'exigence de proportionnalité qui dérive de cette disposition et qui impose aux autorités publiques d'en faire assez sans en faire trop lorsqu'ils tentent de sauvegarder d'autres intérêts légitimes.

Van Enis, Q. (2013). Les mesures de filtrage et de blocage de contenus sur l'internet: un mal (vraiment) nécessaire dans une société démocratique ? Quelques réflexions autour de la liberté d'expression. Rev. trim. dr. h., n°96, 859-886.

Vie privée et protection des données à caractère personnel

Van Gyseghem, J., de Terwange, C., Herveg, J. and Gayrel, C.

Le présent ouvrage est consacré à la protection de la vie privée et des données à caractère personnel. Dans l'approche suivie, il ne s'agit pas de proposer au lecteur un précis sur le droit au respect de la vie privée dans son ensemble. La matière est en effet tentaculaire et un tel ouvrage devrait couvrir le droit à l'intégrité physique et morale, au nom à l'honneur, à l'image, à une vie familiale, à un environnement sain, et la liste est loin d'être close. L'objectif de cet ouvrage consiste plutôt à mettre à disposition des praticiens et de toute personne confrontée à des questionnements liés à la protection des individus face aux développements techniques et sociétaux et à la tournure que prend notre société, un outil apportant les réponses juridiques à de tels questionnements.

Van Gyseghem, J., de Terwange, C., Herveg, J. and Gayrel, C. (2013). Vie privée et protection des données à caractère personnel. Politeia.

"To Shut Down, Push Start": Sixth in Series of Judgments in Belgian Yahoo Case Goes Back to Square One

Verbruggen, F.

Critical analysis on a decision of the Antwerp court of appeals from 2013, in which it convicted a US based electronic service provider for failure to heed a Belgian local prosecutor's direct order to hand over data concerning e-mail-use. The author first wonders whether under Belgian law the type of information requested, actually required a judicial warrant rather than a decision from a prosecutor. Subsequently, he questions the conclusion of the court: that the matter was of a purely Belgian territorial nature and that therefore international law on mutual legal assistance and US law were irrelevant. The author advocates a less unilateral approach to criminal jurisdiction claims over internet operators in a cross-border context and stresses the urgency in replacing traditional MLAT-bureaucracy by more workable tools for law enforcement.

Verbruggen, F. (2014), 'Om af te sluiten, druk op Start': zesde rechter in Belgische Yahoozaak schaart zich achter eerste, Computerrecht, 129-140.

B-CCENTRE-ICRI contribution to London International Cyber Conference, London, 1-2 November 2011.

On 1-2 November the UK hosted the London International Cyber Conference to discuss norms of acceptable behaviour in cyberspace and to build the broadest possible international consensus around basic standards of behaviour which will enhance security and confidence in the networked world, i.e. on how to realise the benefits of cyberspace. The British Government wanted to start the dialogue between major actors in cyberspace, involving industry, academic experts and representatives of civil society. The conference attracted representatives of more than 80 governments and international organisations. The then Belgian Minister of Foreign Affairs, Vanackere reacted in a constructive manner to this initiative, willing to contribute actively to the conference. In order to prepare the Belgian input, the Ministry of Foreign Affairs collected feedback and input from the academic world and civil society to feed the Belgian contribution. B-CCENTRE contributed with argumented considerations regarding the *Trade-off between ensuring a high level of security for citizens and preserving their fundamental rights, such as the right to privacy,* as feedback on a UK 'food for thought' paper sent to the participants which contained already 7 principles which could be the core of the norms to be established by international consensus. The B-CCENTRE input was appreciated by the Belgian delegation to the Conference.

Trade-off between ensuring a high level of security for citizens and preserving their fundamental rights, such as the right to privacy.

F. Coudert

This brief paper highlights the threats posed to privacy by the methods and tools used by law enforcement agencies when fighting cybercrime. It also tries to show that privacy and security should not be approached as conflicting values but rather as mutually reinforcing ones insofar as they both tend to the same objective, namely the protection of Freedom. The challenge however resides in turning this vision into reality. To that end, three action tracks are put forward: (1) at policy level, best practices developed should contain the commitment of public authorities to fully take into account the criteria developed by the ECtHR case law under article 8 (right to privacy) into the legislative framework directed to the fight against cybercrime; at technology level, two approaches should be fostered, (2) the one of "privacy-by design" that looks at limiting the impact of a given technology on individuals' right to privacy from the design phase of such technology, and (3) the one of "accountability-by-design" that pretends to integrate in the technology accountability mechanisms that will enable its users to demonstrate they have acted in full respect with individuals' fundamental rights. All three mechanisms are intended to foster trust.

1. Problem statement: to what extent is privacy challenged in policies fighting against cybercrime.

The pervasive, ubiquitous and invisible nature of cybercrime requires law enforcement to use investigation methods with similar characteristics. In order to adequately answer these new threats, law enforcement agencies should make use of powerful new technologies such as data mining and matching tools that use statistical methods to extract characteristics or tendencies in human behaviour, and foster collaboration, resulting in an increase in the information exchange between these agencies and with the private sector.

Opaque and proactive technologies. The use of the aforemetioned technologies improves the efficiency of investigation methods, e.g. by increasing the rate of crime detection through intelligent software

detecting identity fraud or suspicious financial transactions. They however enable more intrusive practices such as targeted surveillance, investigation or use of search powers.[2]

These technologies are mainly characterized by two prevalent features: their opaqueness to the people being monitored and their proactive nature. The fight against cybercrime requires law enforcement agencies to evolve their traditional operative methods based on reaction to crimes and focused on the gathering of conclusive evidence of wrongdoing 'beyond reasonable doubt' to put before a criminal court[3], towards proactive surveillance that targets the (alleged or potential) criminal and not the crime[4]. Proactive surveillance makes use of methods taken from the Insurance sector and managerial philosophy where data analysis and crime intelligence are pivotal to an objective, a decision-making framework that facilitates crime and problem reduction, disruption and prevention[5]. Both methods have always existed in policing practices but new technologies allow an increase in scale and thus in the intrusiveness of the surveillance performed. This also directly affects the role of the police operative because of the increased automation of surveillance systems where 'the human component is being limited to construction and evaluation roles, with decision-making carried out by computer software through mathematical codes.´[6]

These new investigation tools require the collection of (personal) data in an unrestricted way, not always linked to specific and predefined purposes but rather to cover the mere possibility that these data may become useful at some (undefined) point. Such is for instace the case of the new data retention policies as implemented under Directive 2006/24/EC, the so-called Data Retention Directive[7].

Increase exchange of information. A second threat to privacy is to be found in the increase of personal data exchange between law enforcement agencies. This phenomenon is fostered by two paralell trends: (a) the internationalisation of security threats that require an increased coordination of law enforcement agencies and (b) the expansion of the concept of Security which leads to a progressive (re)integration of the tasks and functions of law enforcement agencies, security services and intelligence agencies[8] which ultimately results in increasing overlaps, in the blurring of organisation boundaries and in the integration of databases. As a way of example, cross-border police cooperation becomes central in the Communication on the Stockholm Programme: better exchange of information is identified as one essential policy goal for the EU in the AFSJ. [9] This is furthermore reinforced by the fostering of information sharing practices, not any more relying on a voluntary basis such as under Interpol, Schengen, Europol and Eurojust Conventions, but rather on an obligation to make available information on an automatic basis under the principle of availability, for instance implemented under the Treaty of Prüm[10]. The principle

[2] CROSSMAN G. et al., Overlooked: Surveillance and Personal Privacy in Modern Britain, Liberty, 2007.
[3] Institute for Prospective Technological Studies, *Security and Privacy for the Citizen in the Post-September 11 Digital Age: a prospective overview*, July 2003, p.99.
[4] NORIS C., *The Intensification and Bifurcation of Surveillance in British Criminal Justice Policy*, Eur J Crim Policy Res (2007) 13:139–158, 2007.
[5] See in that sense, RATCLIFF J.H., *Intelligent-led policing*, In; Wortley, R, Mazerolle, L, and Rombouts, S (Eds) Environmental Criminology and Crime Analysis (Willan Publishing: Cullompton, Devon), 2008.
[6] WOOD D., *The Evolution of Algorithmic Surveillance and the Potential for Social Exclusion, 2003*, as quoted in BROWN I. , KORFF D. , *Privacy and Law Enforcement*, UK Information Commissionner study project, Foundation for Information Policy Research, 2004.
[7] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, OJ L 105 13.04.2006 p. 54
[8] GREENWOOD D. and HUISMAN S., *Transparency and Accountability of Police Forces, Security Services and Intelligence Services*, George C. Marshall Association / DCAF, 2004.
[9] HUSTINX P. , *Data protection and the need for an EU Information management Strategy*, Speech delivered at the first meeting under Swedish Presidency of the Council Ad Hoc Working Group on Information Exchange, 2009, Brussels.
[10] The Treaty of Prüm was incorporated to the European framework by the Council Decision 2008/615/JHA of 23 June 2008 on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime´, OJ 2008 L 210, 6 August, 2008.

of availability[11] ´*entails that information needed for the fight against crime should cross the internal borders of the EU without obstacles*´[12].

Increases in information exchange are not limited to law enforcement agencies but also take place between these agencies and the private sector. Information gathered in the course of the private sector activities is further requested for purposes of fighting against cybercrime. The tracking of Internet users' activities becomes pivotal in order to solve crimes such as pedophilia or identity theft but requires the active involvement of Internet Service Providers. Whereas it helps law enforcement agencies with the investigation of crimes, it also subjects individuals to a detailed monitoring of their daily activities. Private-public partnership is not new, at least in the field of law enforcement, but its impact on citizens is reinforced by the use of data mining technologies that aggravates the pervasive nature of the surveillance.

2. The importance to respect fundamental rights such as the right to privacy when deploying policies to fight cybercrime to secure cyberspace as a trusted environment.

As stressed in the UK paper, cyberspace should be secured as a trusted environment. Only if the right balance is struck between the need for Security and the need to respect fundamental rights, such as the right to privacy, can this trust be constructed.

Security and privacy are often presented as the two faces of the same coin continuously influenced by external factors.[13] In words of the Institute for Prospective Technological Studies (2003), "*if for some reason the perceived need for individual and collective security increases, emphasis on the maintenance of privacy tends to decrease*."[14] Since 9/11, emphasis has however been put on the increase of Security through the use of new technologies often without proper prior debate about their societal implications, particularly in terms of fundamental rights. Privacy is often presented as a mere obstacle to the implementation of more efficient Security practices.

Deciding on the opportunity to deploy a certain technology, on the goals this technology is expected to meet or on its legitimate conditions of use should however necessarily go through a prior societal debate where the impact on fundamental rights is carefully assessed. Taken the example of the introduction of video surveillance and face recognition systems into public places, Browyer (2004) identifies three questions that should be answered before deciding their deployment, namely: "*1) when or whether a sophisticated high-tech application works well enough to be worth deploying, 2) which elements of privacy are essential and which are inessential, and 3) what level of increased safety can come through the introduction of this technology*."[15]

To answer these questions, the metaphor of balancing of interests is often used. This has however been criticized by several scholars, all pointing out the fact that it inevitably leads to a "zero-sum game", incapable of providing satisfying solutions.[16] The debate would thus consist in assessing how much 'liberty' could be lost and how much security is consequently gained. In words of Bowyer, "*the full depth and meaning of Benjamin Franklin's warning about trading liberty for security is not always appreciated. He posted the tradeoff as one giving up "essential liberty" in order to obtain "a little temporary safety". Thus*

[11] European data Protection Authorities, *Declaration on the Principle of Availability, with Common Position and Checklist*, adopted on 11 May 2007, Spring Conference of the European Data Protection Authorities, Cyprus, 10-11 May 2007.
[12] European Data Protection Supervisor, Opinion on the Proposal for a Council Framework Decision on the exchange of information under the principle of availability, COM (2005) 490 final, 17 May 2006.
[13] COUDERT, Fanny (2010) When video cameras watch and screen: Privacy implications of pattern recognition technologies, Computer Law & Security Review 26 (2010), Issue 4, 377-384
[14] Institute for Prospective Technological Studies. Security and privacy for the citizen in the post-September 11 digital age: a prospective overview; 2003.
[15] Bowyer KW. Face recognition technology: security vs. privacy, IEEE Technology and Society Magazine; Spring, 2004
[16] see e.g. Hayes B. There is no "balance" between security and civil liberties - just less of each. In: Essays for civil liberties and democracy in Europe. Essay, no. 12; 2006, ECLN.org; 2006

we can expect that much of the disagreement in this area comes down to whether the increase in safety is judged to be little or much, and temporary or permanent.'[17]

A more positive understanding of the terms of the debate should be preferred. Privacy and Security should be considered as mutually reinforcing values working together towards the same goal, namely contributing to a greater level of Freedom. In that sense, WALLACH for instance suggests considering human rights as an ethic of power. In words of this author, '*every exercise of political power entails two elements. First, it presupposes the need to overcome an extent social conflict or difficulty facing human beings and citizens. As such, the exercise of political power is essentially contested. Second, a purpose always informs the exercise of political power, and that purpose signifies a relationship to an ideal community. While the purpose for which power is exercised does not inherently belong to the fact of its exercise, power without a purpose is sheer force. Insofar as the purpose of power is justified as a social practice, that purpose comprises an 'ethics''*[18]*.*

3. How to implement cybercrime practices respectful of privacy

The challenge however resides in realising this greater Freedom for citizens in practice, i.e. a greater level of Security while adequately protecting their privacy. Several aspects should be considered.

First of all, at level of policy making, a series of criteria should be taken into account where drafting Cybercrime legislation. These criteria have been elaborated through the years by the European Court of Human Rights (hereafter, 'ECtHR') through its case law on article 8.2 (right to privacy) in order to ensure the foreseeability of law enforcement practices and to prevent abuses of power. Article 8§2 explicitly admits as legitimate aims of derogation motives such as national security, public safety, the prevention of disorder or crime or the protection of the rights and freedoms of others. Such derogation should however be 'in accordance with the law' and 'necessary in a democratic society', i.e. 'relevant and sufficient' and proportionate. The case law of the ECtHR has mainly focused on the verification of the first criteria, 'in accordance with the law', giving way to the development of a detailed jurisprudence on the requirements a law should meet to qualify as foreseeable and accessible. The law should install clear, detailed rules governing the scope and application of measures, as well as minimum safeguards concerning duration, storage, usage, access of third parties, procedures for preserving the integrity and confidentiality of data and procedures for its destruction, thus providing sufficient guarantees against the risk of abuse and arbitrariness. The Court has developed the following minimum safeguards that should be set out in statute law in order to avoid abuses of power in the context of telephone tapping, secret surveillance and covert intelligence-gathering and later on extended to strategic monitoring, namely : a) the nature of the offences which may give rise to a surveillance measure; b) a definition of the categories of people liable to be subject to such surveillance; c) a limit on the duration of the surveillance; d) the procedure to be followed for examining, using and storing the data obtained; e) the precautions to be taken when communicating the data to other parties; and f) the circumstances in which recording may or must be erased or the tapes destroyed. The proportionality of the measures should also be carefully assessed. In the Marper case (2008)[19], where the ECtHR had to assess the conformity of the collection and storage of fingerprints, cellular samples and DNA profiles for crime prevention purposes with article 8 ECHR, the Court recalled that '*any State claiming a pioneer role in the development of new technologies bears special responsibility for striking the right balance in this regard'*. The Court further observed that the protection afforded by Article 8 would be unacceptably weakened if the use of modern scientific techniques in the criminal justice system were allowed at any cost and without carefully balancing the potential benefits of the extensive use of such techniques against important private-life interests.

[17] Bowyer KW. Face recognition technology: security vs. privacy, IEEE Technology and Society Magazine; Spring, 2004
[18] WALLACH J.R. , *Human Rights as an ethics of power*, in Human Rights in an Age of Terror, WILSON R.A. (ed.), Cambridge, 2005.
[19] S and Marper v United Kingdom 30562/04 [2008] ECHR 1581 (4 December 2008).

Another track of action should focus on the design of the technologies used by law enforcement authorities to fight cybercrime. These technologies should integrate, from the design phase, features that limit the impact on individuals' privacy. This means that while developing a new technology, its impact on privacy is first assessed to be able in a second time to adopt technological or organisational measures as to limit this impact. This approach is being fostered by the European Commission within the FP7 Security calls which has given a prevalent role to "privacy-by-design" technologies.

However, privacy cannot be fully protected nor trust fully realised if transparency mechanisms that ensure oversight over opaque cybercrime practices, i.e. that privacy safeguards are actually enforced. S. SIMITIS for instance believes that "only the greatest possible transparency under the rule of law [...] ensures that the danger of slipping into a surveillance state can be countered".[20] This is in part because trust, intimately linked with transparency, is essential to a democratic society. As argued by Liberty,

> where surveillance put[s] the privacy of an individual at risk, the broader relationship between the citizen and state is also at stake [insofar] there would be a society where the dignity of the individual has been compromised; intimacy between people, confidence between people and trust in big institutions, whether it is the Health Service or the Government, would be lost.[21]

Transparency can first be realised by ensuring an external and independent oversight. Other forms of *a priori* control over the processing, such as prior checks conducted by data protection authorities (see Section 3.1 above), may form a first step in making them more transparent and thus creating trust. However, trust can only be achieved by ensuring that the "watchers are watched", e.g. by empowering trustworthy authorities to conduct investigations and to report on the findings. Data protection authorities are generally trusted by the public, and have proved to have sufficient independence and knowledge to carry out this role.

Transparency can also be integrated to the technology, including features that will make law enforcement agencies accountable. This concept has been coined as 'accountability-by-design'[22] and comes to complement the one of 'privacy-by-design'. Whereas the first concept seeks to limit the impact of the technology designed on privacy, the later one focus on the enforceability of these measures. Accountability by design is expected to ensure trust by enabling law enforcement agencies to demonstrate that they have acted in full respect with fundamental rights and by easing the detection of malicious or improper uses. This concept is however new and needs to be further explored.

4. Recommendations

- Approach Security and Privacy as mutually reinforcing values that should work together towards the same end, enabling Freedom.
- Introduce into the best practices the need for policy makers to fully implement the criteria developed by the European Court of Human Right under article 8.2. Recall that these criteria are expected to ensure the foreseeability of law enforcement agencies and to limit abuse of power
- Foster "privacy-by design" and "accountability-by design" methodologies for the design of new technologies that will be used to fight against cybercrime. Whereas "privacy-by-design" methodology intends to limit the impact on individuals' privacy of this technology, "accountability-by-design" aims to ensure a greater level of transparency in technologies which are each time more opaque to individuals.

[20] As quoted by the Foundation for Information Policy Research, "UK Information Commissioner study project: privacy and law enforcement, Paper n°4: the legal framework, an analysis of the constitutional European approach to issues of data protection and law enforcement", February 2004, p. 59.
[21] Liberty, *Overlooked: Surveillance and Personal Privacy in Modern Britain*, October 2007, available online at: http://www.liberty-human-rights.org.uk/issues/3-privacy/pdfs/liberty-privacy-report.pdf.
[22] The term "accountability-by-design" has been coined by Matthias Pocs, LLM, in "Accountability-by-design. Example of future biometric systems for crime prevention" paper presented at the PATS, Privacy and Accountability Conference Berlin, 5-6 April 2011

Full Text Articles

"Locating criminal investigative measures in a virtual evironment. Where do searches take place in cyberspace"

C. CONINGS*

Introduction

The territoriality principle limits state sovereignty and its accompanying competencies to a national territory. Likewise, a government's authority to investigate criminal acts is restricted to the territory falling under the competencies of such government. If a government wants to perform investigative acts abroad, it must rely on an official request for legal assistance if no international agreement for cooperation applies. It is often difficult, however, to establish the place where a government exercises its investigatory powers. Whilst few problems regarding procedural competencies arose in the past, digitisation has raised a number of questions relating to the meaning and the correct definition of the concepts of territoriality and sovereignty. What role can territoriality play in a world where physical boundaries are becoming increasingly blurred? Does such blurring necessarily mean that legal territorial boundaries are also becoming blurred? Where should investigative acts be located in a world in which physical distance only plays a limited role? How is sovereignty to be understood in a world that is increasingly becoming a global community? In short: How should we approach sovereignty and territoriality in the current digitised society? Can these concepts still fulfil their original functions or do we need new criteria to define and limit the competencies of investigating authorities in a virtual environment?

I. Traditional approach to territoriality under pressure

1. Origin: State sovereignty and its territorial delineation

1. LEGITIMACY OF THE STATE SOVEREIGNTY - State sovereignty was originally legitimised by the need to organise a community and the idea that the task of maintaining order should be vested in a higher authority that is able to offer its subjects protection.[1] To allow the higher authority to fulfil its task of maintaining order and providing protection, its sovereign power has, among others, the competence to enact laws and enforce them.[2] The idea that a higher authority is in the best position to protect the interests of its subordinates in their mutual relationship (*internal protection*) constitutes an important foundation for state sovereignty. [3] Sovereign authority is only possible if it is adequately recognised by the persons falling under the sovereign competences (bottom-up recognition). Hence, if only few subjects recognise the sovereign authority of the state, the state runs the risk that its sovereignty will be undermined. Consequently, to a certain extent, sovereignty relies on *internal recognition* by its subjects.

2. ESSENTIAL (TERRITORIAL) DELINEATION - The territoriality principle restricts state sovereignty and its accompanying competencies to a national territory. Only by limiting sovereignty in a certain way is it possible to constitute inter-state recognition, i.e. *external recognition.* This constitutes a second form of recognition, which is also an essential prerequisite for state sovereignty.[4] The limitation is aimed at

---

* The author is PhD candidate at the Institute for Criminal Law of the University of Leuven and affiliated researcher at the B-CCENTRE. This contribution has already been published in Dutch in *Nullum Crimen* 2014, no. 1, 1-25.

[1] We can trace this idea back to Social Contract thinkers such as THOMAS HOBBES, JOHN LOCKE, JEAN-JACQUES ROUSSEAU and JOHN RAWLS, for example.

[2] A. CASSESE, *International Law,* Oxford, Oxford University Press, 2005, 49-50.

[3] E. LANCKSWEERDT, "Soevereiniteit, angst en leiderschap", *TBP* 2012, 472. The author thereby refers to THOMAS HOBBES, one of the most prominent founders of the theory of sovereignty.

[4] I. WALLERSTEIN, *World-Systems Analysis: An Introduction*, Durham, Duke University Press, 2004, 44: *"Sovereignty is more than anything else a matter of legitimacy [...that] requires reciprocal recognition. Sovereignty is a hypothetical trade,*

protecting the sovereignty as such and enabling peaceful international co-existence.[5] The UN Charter mentions the sovereign equality of states in this context.[6] The limitation comes to expression in the authority of a state to exclude other states from exercising sovereign powers within its territory.[7] In this way, the sovereign state can also guarantee that the persons and goods within its territory are protected against unlawful interference by other sovereign states (*external protection*).[8] Protection against infringements by persons who are on the territory of another state is provided by international cooperation between the respective sovereign states.[9] This is the only way in which sovereign states can fully accomplish their task.

Territoriality proved to be the most practicable and logical criterion to delineate state authority.[10] State competence extends in the first place to the national territory, territorial waters and the airspace above them.[11] Because of common interest, the high seas (*mare liberum*) and space are free of sovereignty claims.[12] Consequently, No state has the right to exclude other states from space or the high seas. Both spheres may be used by any state whatsoever.[13] Yet, certain "territorial" delineation can be found in space and in the high seas. For instance, ships sailing in high seas and objects launched into space, do fall under the jurisdiction of the state whose flags they bear or where they were registered.[14] Although space and the high seas, as such, are free of individual jurisdiction, states can consequently still have sovereign competence over events taking place in these areas.

3. INTERNAL RECOGNITION OF TERRITORIAL DELINEATION – As is the case with state sovereignty, where (subjects') internal recognition applies, there is also a form of internal recognition of the territorial delineation of such sovereignty. Legal subjects recognise the co-existence of various societies, each of which allocates sovereign competence to a higher body in order to organise and protect the society. They, therefore, also acknowledge that the sovereignty of their own state, which is aimed at providing them with legal protection, must necessarily be limited. This entails that subjects are aware of the consequences of crossing the national borders and accept these consequences. In fact, they recognise that they are entering the sovereign competence of another state every time they traverse the border, knowing that such an act implies relinquishing the protection offered by their own state. Likewise, they accept that the goods they take with them across the border fall under the sovereign competence of the state they are visiting. The visited state must fulfil its protective task in respect of all persons entering its territory. Such persons are, therefore, required to adhere to the local regulations.
Every state can enforce its laws and exercise the necessary law enforcement competencies in respect of persons who enter its territory. Consequently, if one does not wish to subject oneself or one's goods (e.g. laptop, accounting and medical file) to the competencies of a foreign state, one must stay within the boundaries of one's own country or leave one's goods there. The recognition of the sovereignty's

in which two potentially conflicting sides, respecting de facto realities of competency, exchange such recognitions as their least costly strategy."

[5] W.H. VON HEINEGG, "Legal implications of Territorial Sovereignty in Cyberspace", in C. CZOSSECK, R. OTTIS, K. ZIOLKOWSKI (eds), *4th International Conference on Cyber Conflict,* Tallinn, NATO CCD COE Publications, 2012, 8.

[6] Article 2 of the United Nations Charter.

[7] A. CASSESE, *International Law,* Oxford, Oxford University Press, 2005, 51.

[8] W.H. VON HEINEGG, "Legal implications of Territorial Sovereignty in Cyberspace", in C. CZOSSECK, R. OTTIS, K. ZIOLKOWSKI (eds), *4th International Conference on Cyber Conflict,* Tallinn, NATO CCD COE Publications, 2012, 8.

[9] In addition, external recognition of sovereignty is accompanied by an obligation of states not to allow their territory to be used for acts contrary to the rights of other states. They must therefore use all the means at their disposal in order to avoid such use. PCIJ, 9 April 1949, *The Korfu Channel Case*, http://www.icj-cij.org/docket/files/1/1645.pdf; W.H. VON HEINEGG, "Legal implications of Territorial Sovereignty in Cyberspace", in C. CZOSSECK, R. OTTIS, K. ZIOLKOWSKI (eds), *4th International Conference on Cyber Conflict,* Tallinn, NATO CCD COE Publications, 2012, 15 et seq.

[10] See extensively in this regard: A. CASSESE, *International Law,* Oxford, Oxford University Press, 2005, 81 et seq.

[11] In more specific terms, see: C. VAN DEN WYNGAERT, *Strafrecht en strafprocesrecht en internationaal strafrecht,* Antwerpen, Maklu, 2006, 1205 ff; W. DEREZE, "De grens tussen luchtvaart en ruimtevaart"*, Jura Falconis* 2007-08, 100-104.

[12] W. DEREZE, "De grens tussen luchtvaart en ruimtevaart"*, Jura Falconis* 2007-08, 102-104; M. HILDEBRANDT, "Extraterritorial jurisdiction to enforce in cyberspace?: Bodin, Schmitt, Grotius in cyberspace", *University of Toronto Law Journal* 2013, afl. 63, 196-224.

[13] UN Outer Space Treaty of 27 January 1967; UN Convention on the Law of the Sea of 10 December 1982.

[14] C. VAN DEN WYNGAERT, *Strafrecht en strafprocesrecht en internationaal strafrecht,* Antwerpen, Maklu, 2006, 1206 ff; W. DEREZE, "De grens tussen luchtvaart en ruimtevaart"*, Jura Falconis* 2007-08, 102-104.

territorial delineation creates legal certainty. The legal system applicable to a person or item is in the first place that of the state where that person or item is located.

4. LEGAL PROTECTION – SOVEREIGNTY – TERRITORIALITY – When considering the application of the principles of sovereignty and territoriality in the current digitised society, one must keep in mind the outlined interplay between legal protection, sovereignty and territoriality. We therefore briefly summarise the above as follows: (1) State sovereignty is aimed at responding to the primary need for maintaining order and providing protection within a community; (2) The recognition that a higher authority is in the best position to fulfil this original need is one of the most important foundations of state sovereignty (internal recognition). In its turn, sovereignty is protected by its territorial delineation. (3) Such delineation actually enables other states to recognise the state's sovereignty (external recognition). (4) In addition, it ensures that the sovereign state can fulfil its protective function by also offering protection against actions by other sovereign states within its territory (external protection); (5) Finally, legal subordinates also recognise the necessary territorial limitation of sovereign authorities.

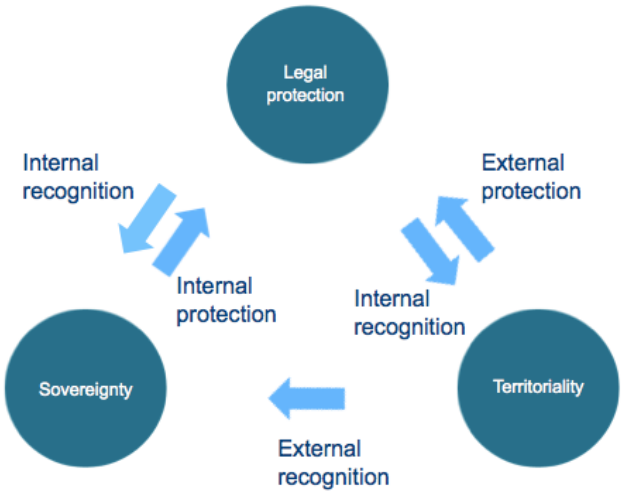


Figure 1: Interplay between legal protection, sovereignty and territoriality.

5. CENTRAL QUESTION - Below we first consider how the law traditionally defines the territoriality principle. We then outline how the modern phenomenon of "cyberspace" challenges the traditional paradigm. In this regard, we are focusing on Criminal Procedure Law, in particular on regulations relating to criminal law searches. The question we finally wish to answer is the following: Can we *territorially delineate* the current (virtual) investigative possibilities in such a way that (internal and external) *sovereignty* and therefore the (internal and external) *protection of* individuals' *fundamental rights* are guaranteed? In other words, can we interpret the territoriality principle in such a way that the interplay outlined above remains intact? If not, the territoriality principle loses its validity in the virtual environment and a new criterion will have to be sought.

2. Determining location in traditional Criminal Law and Criminal Procedure Law

6. DETERMINING LOCATION IN SUBSTANTIVE CRIMINAL LAW – Firstly, the principles of sovereignty and territoriality play a role in substantive criminal law. Sovereignty entails the competence to enact criminal laws and to impose penalties for transgressions.[15] Based on the territoriality principle, these laws primarily apply to persons and objects within the territory of the enacting state.[16] For instance, in principle, Belgian Criminal

[15] E. LANCKSWEERDT, "Soevereiniteit, angst en leiderschap", *TBP* 2012, 471.

[16] With regard to Belgium, see: Article 3 of the Criminal Code: "*Crimes committed by Belgians or foreign nationals on the territory of the Kingdom, is punished in accordance with the provisions of Belgian laws*." Furthermore, states can also provide for an extra-territorial application of the Substantive Criminal provisions to the extent that this is not prohibited by International Law (PCIJ 7 September 1927, *SS Lotus* (France/Turkey), *C.P.J.I.Rec.* 1927, Series A, no. 10.). Possible foundations for an extra-territorial application are the principles of active and passive personality, the

Law applies to crimes that are committed on Belgian territory. However, it is not always easy to unequivocally establish the place where a crime has been committed. The act may, for instance, be committed in one country, while the consequence (required to constitute the crime) is situated in another country. Or, the crime may consist of several constitutive acts that take place on more than one territory. To counter this problem, several locating principles[17] have been developed in jurisprudence and doctrine, which should allow to determine whether or not a crime was committed on national territory.[18]

7. DETERMINING LOCATION IN FORMAL CRIMINAL LAW – Secondly, sovereignty and territoriality are key notions in Criminal Procedure Law as well. Law enforcement competencies and the state's monopoly on the use of force stem from the state's sovereignty.[19] Again territoriality forms an important criterion in limiting these competencies. In principle, national investigating authorities can only perform investigative acts on national territory.[20] In contrast to the situation in Substantive Criminal Law, the lack of legal criteria for the purposes of locating investigative acts was generally not experienced as problematic in the past. A person is detained where he is to be found; physical evidence is collected where the evidence is to be found. However, there may be situations in which the location of investigative acts is unclear. This would be the case where, For example, the location of the evidence is not the same as the location from where the evidence can be perceived. For instance, do we need to consider an observation to be cross-border when the person being observed is abroad or only when the officer performing the observation crosses the border? Issues regarding the precise location of an investigative act will occur more and more due to the fact that computer systems such as satellites[21], GPS systems[22] and smartphones[23] will probably be used more frequently for investigative purposes. Another problem arises when the evidence itself is difficult to locate. Telecommunication is one such example. Where does one locate an intercepted conversation (the sought information)? At the location of the receiver or rather the location of the sender? At the location of both parties or at the premises of the Telecommunication provider? Consequently, which

protection principle and the universality principle. See extensively in this regard: C. RYNGAERT, *Jurisdiction in International Law*, Oxford, Oxford University Press, 2008, 85, et seq.

[17] Cf. *the theory bases on the activity criterion* where the place where the perpetrator's physical act took place is the decisive factor in determining where the crime was committed; *the theory based on the criterion of the instrument of the crime*, where the place where the instrument used is the determining element; *the theory based on the criterion of the constitutive consequence* according to which the place where the constitutive consequence occurred is the place of the crime; *the theory based on the ubiquity criterion*, according to which a crime is committed in any place where a constitutive element thereof occurs and the *theory based on the criterion of the effect*, whereby even further removed results can have an influence on locating a crime.

[18] P. DE HERT, "Cybercrime and Jurisdiction in Belgium and the Netherlands. Lotus in Cyberspace - Whose Sovereignty Is at Stake?" in X, *Cybercrime and Jurisdiction. A Global Survey,* Den Haag, T.M.C. Asser Press, 2006, 96; C. VAN DEN WYNGAERT, *Strafrecht en strafprocesrecht in hoofdlijnen,* Antwerpen, Maklu, 2011, 143 ff; H. WOLSWIJK, *Locus delicti en rechtsmacht,* Deventer, Gouda Quint, 1998, 353 p.; T. VANDER BEKEN, *Forumkeuze in het international strafrecht,* Antwerpen-Apeldoorn, Maklu, 1999, 486 p.

[19] E. LANCKSWEERDT, "Soevereiniteit, angst en leiderschap", *TBP* 2012, 471.

[20] PCIJ 7 september 1927, *SS Lotus* (Frankrijk/Turkije)*, C.P.J.I.Rec.* 1927, Serie A, no. 10, consideration 45 ("*Now the first and foremost restriction imposed by international law upon a State is that – failing the existence of a permissive rule to the contrary – it may not exercise its power in any form in the territory of another State. In this sense jurisdiction is certainly territorial; it cannot be exercised by a State outside its territory except by virtue of a permissive rule derived from international custom or from a convention.*"); P. DE HERT, "Cybercrime and Jurisdiction in Belgium and the Netherlands. Lotus in Cyberspace - Whose Sovereignty Is at Stake?" in X, *Cybercrime and Jurisdiction. A Global Survey,* Den Haag, T.M.C. Asser Press, 2006, 102; B.J. KOOPS, R. LEENES, P. DE HERT, S. OLISLAEGERS, *Misdaad en opsporing in de wolken, knelpunten en kansen van cloud computing voor de Nederlandse opsporing* in *WODC,* Tilburg, Universiteit van Tilburg, 2012, 36; T. LAUREYS, *Informaticacriminaliteit: actuele wetgeving, tekst, analyse en bronnen*, Gent, Mys & Breesch, 2001, 70; H. SPANG-HANSSEN, *Cyberspace & International Law on Jurisdiction,* Kopenhagen, DJØF Publishing, 2004, 267.

[21] Satellites are currently already being used to maintain law and order, e.g. for Environmental Law purposes. See M.S. ARANZAMENDI, R. SANDAU, K. SCHROGL, *"Current Legal Issues for Satellite Earth Observation",* ESPI report 25, ESPI, Vienna, http://www.espi.or.at. However, technological developments provide a continual improvement of image resolution. Therefore, satellites may well be used in more fields in the future, if required. The issue regarding location will therefore become all the more relevant in the future.

[22] See, e.g. ECHR 2 September 2010, no. 35623/05, Uzun/Germany.

[23] See, e.g. explanatory memorandum to the Dutch bill to amend the Criminal Code and the Criminal Procedure Code regarding improvement and reinforcement of the investigation and prosecution of computer criminality (computer criminality law III, May 2013, 20, www.rijksoverheid.nl).

government has the (sovereign) competence to intercept the transborder conversation, subject to the conditions outlined in its national law?

8. LOCATING PRINCIPLES IN CRIMINAL PROCEDURE LAW: WIRETAP – The wiretap allows law enforcement agencies to eavesdrop on conversations. It can be applied even to persons who are conversing between two countries. The communication is sent from the sender to the receiver via technical intermediate stations (e.g. transmission masts), which can, in their turn, be situated on the territory of another state. National legislatures and the European Union seem to be evading the question on locating the evidence (the conversation). [24] In terms of Belgian law, intercepting telephone conversations is simply ordered regarding a person, a place or means of telecommunication. Consequently, the country where said person, place or means is/are located determines where the interception must be located, to whose territory the conversation belongs and thus which authorities are competent to intercept the communication. The European Union approaches this issue in the same manner in the Convention on Mutual Legal Assistance. Apart from the situations where foreign technical assistance is required, the European rules on cooperation in criminal matters only come into effect when the *person whose telephone is to be intercepted* is not (or is no longer) on the national territory of the intercepting state.[25] It seems that the future regulatory framework on the European Investigation Order will not change this.[26] Hence, under European Union rules, a conversation takes place at the location(s) where the participants were at the time of the conversation.[27] In this way, one and the same conversation can be located in different territories and can fall under the sovereign competence of different governments (i.e. if those participating in the conversation are to be found in different countries). The governments do not need one another's permission to intercept a conversation belonging to both of them. In this way, every state has complete authority regarding possible direct interferences in the right to respect for correspondence of the persons located on its territory. Every State determines independently[28] when an intercepting measure is allowed in respect of the persons on its territory and is responsible for protecting the fundamental rights of those persons from unlawful interferences by foreign States (external protection).[29] Criminal Procedure Law therefore apparently also recognises locating principles, although this is less explicit. The focus thereby shifts from the object sought, i.e. the evidence (*object-oriented approach*) to the subject investigated, i.e. the investigated person (*subject-oriented approach*).

9. LOCATING PRINCIPLES IN CRIMINAL PROCEDURE LAW: OBSERVATION – There is no locating principle in supranational or international agreements relating to observation in the physical world. Neither does Belgian national law explicitly determine when an observation transcends a border. Is the decisive factor the place where the person or object observed (subject or object) is to be found, or the place where the

[24] See Article 90 ter §1, paragaph 3 of the Belgian Criminal Procedure Code; Article 126 m of the Dutch Criminal Procedure Code.; §100a Strafprozeβordnung (StPo); Articles 18-20 of the Convention of 29 May 2000 on Mutual Assistance in Criminal Matters between the Member States of the European Union, www.eclan.eu (Referred to hereafter as the EU Convention on Mutual Assistance in Criminal Matters.)

[25] See Articles 18-20 of the EU Convention on Mutual Assistance in Criminal Matters. See also the explanatory report to the Convention of 29 May 2000 on Mutual Assistance in Criminal Matters between the Member States of the European Union, *Official Journal* C 379 of 29 December 2000, no. 379, 20-21. The explanatory report explicitly mentions that a state's interception of communication to or from its territory implies a measure on its own territory.

[26] Proposal for a Directive of the European Parliament and the Council regarding the European Investigation Order in criminal matters, *CEU* 9145/10, 29 April 2010. The proposal only changes the way of cooperation with regard to *real time* evidence gathering. See Articles 3 and 27 of the proposal.

[27] P. DE HERT, "Cybercrime and jurisdiction in Belgium and the Netherlands. Lotus in Cyberspace - Whose Sovereignty Is at Stake?" in X, *Cybercrime and Jurisdiction. A Global Survey,* Den Haag, T.M.C. Asser Press, 2006, 82.

[28] This must however be done while duly respecting the limitations emanating from international obligations that the respective state has undertaken to observe, such as Article 8 of the ECHR.

[29] See Article 18 paragraph 5 a) of the EU Convention on Mutual Assistance in Criminal Matters and the accompanying explanatory report. A Member State of which only technical assistance is requested may not make the granting of the request to intercept communication and the direct passing on of the intercepted information dependent on the question whether said request is in accordance with its national legislation. This situation occurs, for example, if the person whose communication is to be intercepted is to be found on the territory of the state intercepting the communication and uses a satellite telephone. In view of Article 20, paragraph 4 b), a Member State can hinder the interception of the communication of a person on its territory by another Member State, for example, if the interception were not permissible under its own legal system or it would infringe its sovereignty, security, public order or other essential concerns.

person performing the observation is to be found? In our opinion, the location from which the observation is performed cannot, as such, be decisive. In this perspective, the extent to which the observed person is legally protected is completely dependent on the observing state's technical possibilities. At least in the future, it will probably be technically possible to combine infrared technology with satellite technology, for example, so that heat sources in houses can be detected all over the world. If the location of the person observing is decisive, such observation could be performed pursuant to local national legislation, even though the person observed is somewhere else in the world. Conversely, by focusing on the location of the person observed, states retain the possibility of exercising their sovereign monitoring competencies in respect of all actions performed on their territory in accordance with national law. This is the only perspective that allows for the fulfilment of their task of maintaining order and providing protection on their own territory. In addition, this approach enables states, by means of their right to exclusion, to protect persons and objects on their own territory against unlawful infringements of fundamental rights by foreign authorities. Moreover, focusing on the place from where the observation is performed leads to an illogical distinction between observance from the air (e.g. by means of drones), which forms part of the territory of the state located underneath it, and surveillance from space by means of satellites.[30] We are therefore of the opinion that the location of an investigated subject (i.e. the person whose telecommunication is intercepted or the observed person/object) should determine the location of traditional investigative acts *in real time*, such as the wiretap and observation. In our opinion, if states wish to use satellites or other systems to check up on one another's territory, they can only do so on the grounds of international (possible tacit) agreements.[31]

3. Digitisation and the origins of cyberspace

"New communities are being built today.
You cannot see them, except on a computer screen.
You cannot visit them, except through your keyboard.
Their highways are wires and optical fibers;
their language a series of ones and zeroes."[32]

10. DIGITISATION AND DETERMINING LOCATION – Information and communication technology (ICT) has developed enormously during the past decades. Digitisation is an important aspect in this regard and raises new questions regarding the determination of location, within both the scope of Criminal Law and Criminal Procedure Law.[33] After giving an explanation of these developments, we will pursue the issue of determining location in Criminal Procedure Law in further detail.

---

[30] For the difficult distinction between air and space, see: W. DEREZE, "De grens tussen luchtvaart en ruimtevaart", *Jura. Falc.* 2007-08, afl. 1, 99-129.

[31] See for example: The principles relating to remote sensing of the Earth from space, adopted by the General Assembly of the United Nations on 11 december 1986, http://www.un.org/documents/ga/res/41/a41r065.htm: In accordance to those principle remote sensing activities shall be carried out for the benefit and in the interests of all countries. Shared interests are for example the protection of the environment and the protection of mankind from natural disasters.

[32] A. GAFFIN & J. HEITKÖTTER, *Big dummies guide to the internet*, http://www.bsd.org/bdgtti/.

[33] See, for example: S. BRENNER, B-J KOOPS, "Approaches to Cybercrime Jurisdiction", *Journal of High Technology Law* 2004, Vol. 4, 1-46; F. CAJANI, *Technologies and Business vs Law - Cloud computing transborder access and data retention*, www.coe.int; CYBERCRIME CONVENTION COMMITTEE, "Report: Transborder access and jurisdiction: What are the options?", *T-CY* 2012, no. 3, 69 p.; K. DE SCHEPPER, F. VERBRUGGEN, "Can the *Space Invaders* evade our *Pac-Man*? Belgian substantive and procedural criminal jurisdiction in the case of a criminal offence of refusal to cooperate on the part of electronic service providers.", in *B-CCENTRE Report* 2014. M. HILDEBRANDT, M.E. KONING, "Universele handhavingsjurisdictie in cyberspace?", *Strafblad* 2012, afl. 3, 195-203; B-J KOOPS, S. BRENNER (eds), *Cybercrime and Jurisdiction, a global survey,* Den Haag, T.M.C. Asser Press, 2006, 374 p.; N. SEITZ, "Transborder search: a new perspective in law enforcement?", *Yale Journal of Law and Technology* 2005, Vol. 7, 23 ff; J. SPOENLE, *Discussion paper: Cloud computing and cybercrime investigations: Territoriality vs. the power of disposal?,* Project on Cybercrime Council of Europe, 2010, http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/documents/internationalcooperation/2079_Cloud_Computing_power_disposal_31Aug10a.pdf ; P. VAN LINTHOUT, "Territoriale bevoegdheid in cyberspace", *T. Strafr.* 2009, afl. 2, 113-114.

11. DIGITISATION - Digitisation is the translation of information into a language containing only noughts and ones, or what is called the language of bits and bytes, and which is the (universal) computer language.[34] Almost everything can be translated into this binary language. Not only texts and figures, but also sound, still and moving images are increasingly translated into series of noughts and ones (cf. digital cameras).[35] The digitisation of information is accompanied by a number of benefits, one of which is that it is easy to archive large amounts of digital information. Moreover, digital information is easier to work with, copy and move around.[36]

12. THE INFORMATION HIGHWAY - Digital information is transported by means of what is called the "the information highway".[37] The world is currently crisscrossed by an immense network of copper cables, fibreglass, radio waves and satellite signals. These "roads" make it possible to transport information all over the world by means of telephone, fax and internet traffic.[38] Digital information "travels" on the roads, provided for this purpose, from the sender to the receiver, so to speak. So far, there is no additional problem in locating internet traffic as compared to telephone traffic.

13. CYBERSPACE: A GLOBAL COMMUNITY - However, the metaphor of the information highway falls short in light of the possibilities currently offered by the worldwide digital network. The network does not only consist of paths along which users can send and receive information. In addition, users can personally access information (data) that has been stored at certain points along the road (computers and servers) and process that data at any time. The flexible and global network actually makes it possible to use one's computer to access and work with other IT systems.[39] The Internet further makes it possible to transport and keep one's data somewhere else, and access services that are offered at a distance. In all this, neither the Internet user nor the service provider need to travel.

The roads along which digital information is transported have evolved into a place of its own. It has become a platform where information can be offered, fetched and archived. It is now a place where people can contact one another in various virtual ways, look up information (in all possible forms) in cyber libraries, keep information in virtual archives, hold discussions in chat groups, openly voice their opinions on virtual Speakers' Corners, do shopping in cybershops, visit lavishly equipped cyber theme parks and even start living a second life. As such, the roads form part of a larger entity, a second world, a virtual world, which has found its way into homes, schools and offices. It, so to speak, completely encompasses the real world.[40] This is what is called cyberspace.

4. A new procedural locating issue

14. LINK WITH DIFFERENT PHYSICAL LOCATIONS – Everything that happens in cyberspace can be linked to the physical world in several ways. In contrast to traditional telephone communication, conversations and acts in cyberspace (such as emails send by means of webmail applications, remarks and discussions on social media and images and documents stored in the cloud) leave behind traces that are stored with a third person (mostly an Internet service provider). Consequently, information about a person is no longer only to be found in paper files, boxes or hard disks in a person's home or office but also, and increasingly, on servers and computers of these third parties.

---

[34] F. MARAIN & J. MORTELMANS, *Wie doet wat op de informatiesnelweg?,* Groot-Bijgaarden, Scoop, 1995, 15.
[35] J. DUMORTIER (ed.), *Recente ontwikkelingen in media- en telecommunicatierecht,* Brugge, Die Keure, 1996, 25; G.L. HERRERA, "Cyberspace and Sovereignty: Thoughts on Physical Space and Digital Space", 2005, *kms2.isn.ethz.ch,* 4.
[36] See: F. MARAIN & J. MORTELMANS, *Wie doet wat op de informatiesnelweg?,* Groot-Bijgaarden, Scoop, 1995, 15-17.
[37] D. DE GROOF, *Encyclomedia: wegwijs op de informatiesnelweg,* Leuven, Davidsfonds, 1995, 442 p.; J. DUMORTIER (ed.), *Recente ontwikkelingen in media- en telecommunicatierecht,* Brugge, Die Keure, 1996, 25.
[38] The internet is a network of networks, by means of which, by using a computer system, a user has access to an enormous number of other computer networks or connections all over the world. C. UYTTENDAELE, *Openbare informatie. (Public information) Het juridisch statuut in een convergerende mediaomgeving,* Antwerpen, Maklu, 2002, 128; F. MARAIN & J. MORTELMANS, *Wie doet wat op de informatiesnelweg?,* Groot-Bijgaarden, Scoop, 1995, 52.
[39] J. GULDENTOPS, *Geschiedenis en het internet: een historische, methodologische en heuristische benadering van de informatiesnelweg,* Leuven, Acco, 1996, 2.
[40] For more information, see: A. GAFFIN & J. HEITKÖTTER, *Big dummies guide to the internet*, http://www.bsd.org/bdgtti/.

Furthermore, such third persons can also manage their servers at a distance. This entails that the location of the service provider and the place where the data are stored may differ. For example, Facebook is an American service provider, but it can store its data on servers that are located anywhere in the world. To make matters worse, when information is sent to, or requested from, a server, it randomly travels between the user and the storage place. This means that it can also be located at technical intermediate stops (e.g. an Internet Exchange Point (IXP)), albeit only for a limited period of time.[41]

The Internet reality separates the *location of the data* (which can be searched within the scope of a Criminal Law investigation) from the *location of the persons* (whose fundamental rights may be affected by such investigation) in a way never before encountered. The location where data are stored, the location of the consulted service and the location where those data and such service can be used may differ. During the course of an investigation, law enforcement agencies are not necessarily on the territory where the sought information is to be found, neither are they necessarily to be found on the territory where the investigated person or consulted service provider is to be found. As is the case with the users, the law enforcement agencies are also no longer dependent on a specific location.[42]

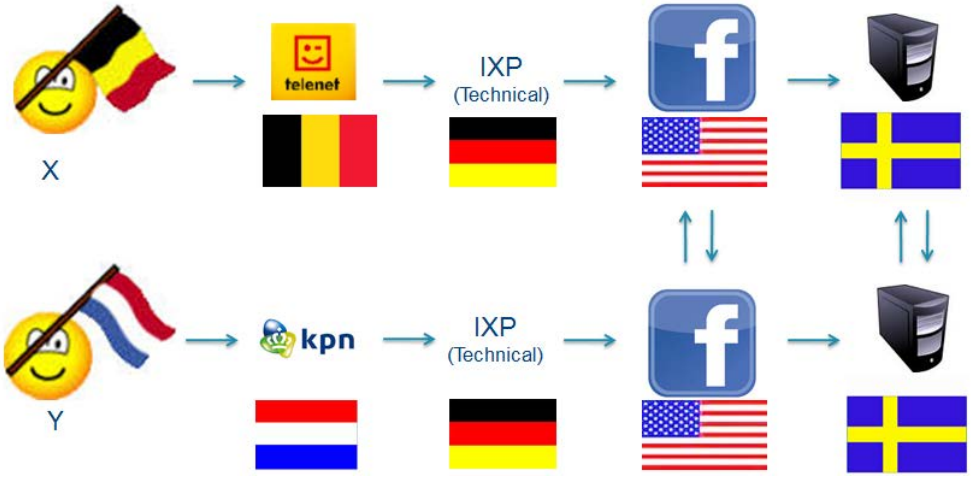


Figure 2: Simplified illustration of the link between online communication (between X and Y) and various physical locations

15. DETERMINING LOCATION? - Consequently, when law enforcement agencies collect evidence in the virtual world (e.g. through looking at a Facebook account, Google calendar, Dropbox account or a YaHoo! webmail account), one of the questions that arises, pertains to the location of their investigative actions. In such a case, is the investigative act located in the territory where the sought data are stored, or is it located in the territory where the investigated person can be found? Is the investigating authority operating in the territory from where they performed the investigative act? Does the location of the service provider play a role in this matter? Each criterion represents a different link between the digital evidence sought and the physical reality. Consequently, each criterion can locate the investigative act on a certain territory. However, the question is: which criterion must be the decisive one?

II. Locating investigative acts in cyberspace

16. TYPES OF SEARCHES – A distinction can be made between two types of searches for evidence in cyberspace. The first involves law enforcement agencies keeping a "virtual eye" on a person in real time (hereafter: *virtual search in real time)*, whilst the second involves a search for stored data, independent of a simultaneous action by the investigated subject (hereafter: *search for stored data).* Virtual search in

[41] See no. 23, below.
[42] M. HILDEBRANDT, "Extraterritorial jurisdiction to enforce in cyberspace?: Bodin, Schmitt, Grotius in cyberspace", *University of Toronto Law Journal*, 2013, afl. 63, 220-221.

real time refers to observing virtual actions such as opening websites, communications or files while those actions are being performed by the investigated subject.[43] Looking into the opened websites, communications and files as such also constitutes investigating in real time. This can also apply to communications from the past, for instance, when the investigated person is looking at them again. Using key loggers[44], which register keyboard keystrokes and mouse movements, is an example of virtual search in real time, as is viewing or listening to communication at the moment at which it is being performed by the investigated subject (e.g. Skype or chat conversation, typing and sending emails). In contrast, the search for stored data is independent of the investigated subject's simultaneous actions regarding the data being investigated. This concerns an (open or covert) search within profiles on social media or accounts providing access to cloud services (e.g. Dropbox or iCloud) or webmail services (e.g. Yahoo!, Hotmail or Gmail). The distinction between the two types of investigative measures is determined by answering the following question: Do law enforcement officers perceive what the investigated person is doing at the moment at which the search is being performed (viewing what is being opened, viewed or listened to, or intercepting a live conversation) or do they look into data independent of a simultaneous action by the subject? In this way, we do not follow the technical distinction currently being applied in Belgium, i.e. the question as to whether or not the data investigated are in transmission. The technical criterion is extremely difficult to use in a digital environment.[45] Furthermore we are of the opinion that it is not a pertinent criterion, not only regarding the distinction between types of searches,[46] but also regarding the issue of locating the investigative acts. (see no. 30, below)

17. Below we consider where each type of search is currently located, and we examine whether such determination of location sustains the outlined interplay between legal protection, sovereignty and territoriality (see no. 4, above). Where it seems that this is not the case, we look for alternative criteria to locate virtual investigative acts. In this way, we attempt to find the main criterion for locating the investigation, both for virtual search in real time and for the search for stored data. We subsequently pose the question whether, within the scope of virtual searches in general, the territorial competence on the grounds of the desired main criterion must be supplemented with the competencies of other states that also show a link with the sought data. Finally, we examine whether the proposed approach can also be used in practice. After all, having a beautiful theory serves no purpose whatsoever if it does not work in practice.

1. Virtual search in real time

A. Current contradictory approach

18. EU CONVENTION ON MUTUAL ASSISTANCE IN CRIMINAL MATTERS – The subject-oriented approach of the EU Convention on Mutual Assistance in Criminal Matters, which we discussed within the scope of the traditional competence to intercept communication (see no. 8, above), also applies to intercepting new types of telecommunication. The explanatory report to the Convention explicitly refers to the intention to apply the provisions of the Convention to the interception of current and future technologies. [47] It also refers to the obtainment of both traffic data (who communicates with whom, at what time, for how long,

[43] This can technically be done by using spyware, for example.
[44] We do not deal with the question whether or not the investigative institutions are allowed to use key loggers. We only consider the question of where investigative actions should be located.
[45] See extensively in this regard: P. VAN LINTHOUT, J. KERKHOFS, "Internetrecherche: informaticatap en netwerkzoeking, licht aan het eind van de tunnel", *T. Strafr.* 2008, 79-94.
[46] In Belgium, there is a strict legal regime for investigating communication *"during the transmission stage"* (Article 90 *ter,* et seq. of the Criminal Procedure Code). This was a logical legislative choice, in view of the fact that at the moment when the legislation on communication interception was created in 1994, the focus was aimed at telephone conversations, whereby one could only obtain knowledge of the *content* of communication while it was in transmission. One could only constitute the *existence* of communication before or after the transmission. Taking due note of the content of the communication obviously constitutes major interference with the right to privacy and therefore needed to be linked to stricter requirements.However, this logic is no longer valid in the digital world.One can also learn about communication content before and after the transmission.
[47] Explanatory report to the EU Convention on Mutual Assistance in Criminal Matters no. 379, 20 and 22.

etc.) and content data.[48] Therefore, according to the Convention, such interception is to be performed in the territory where the person whose communication is to be intercepted is located.

19. CONVENTION ON CYBERCRIME – Articles 20 and 21 of the Convention on Cybercrime[49] oblige signatory states to adopt legislative and other measures to empower their competent authorities to collect or record traffic data[50] and content data relating to specified *communications in their respective territories* that is transmitted by means of a computer system. On the one hand, the states must provide a possibility for competent officials to collect or intercept the data through the application of technical means on their territory.[51] On the other hand, the Convention requires the member states to provide an obligation on service providers to cooperate with those competent authorities. This implies an obligation for service providers to intercept data by technical means on the territory of such state or to assist the authority to do so. According to the explanatory report to the Cybercrime Convention, the obligation to cooperate can, "*in practical terms*", "*generally*" be applied to service providers who have a physical infrastructure or equipment at their disposal on the territory of the state giving the order that enables them to enforce the measure.[52] As is the case for telephone interception, it seems that international rules regarding mutual legal assistance are therefore required when (technical) assistance from abroad is necessary.[53] Articles 20 and 21 only refer to competences relating to communications occurring on the territories of the states. According to the explanatory report, a communication occurs on the territory of a Member State if one of the communicating parties is located on its territory or if the computer system or telecommunication equipment through which the communication is conducted, is located there.[54] Communicating parties can be both persons and computers.[55] This is indicative of the vast meaning of the concept of "communication" in the Cybercrime Convention, which also includes, for instance, opening a website.[56]

20. DISCREPANCY BETWEEN COUNCIL OF EUROPE AND EU - We therefore also find a locating principle in the Convention on Cybercrime, which, in fact, partially corresponds with the locating principle we found in the EU Convention on Mutual Assistance in Criminal Matters. The Convention on Cybercrime confirms the subject-oriented approach of the EU Convention by referring to the location of the communicating parties. There is, however, an important difference between the two. Without additional explanation, the Convention on Cybercrime seems to require that competence to intercept communication must also be

---

[48] Explanatory report to the EU Convention on Mutual Assistance in Criminal Matters no. 379, 22.

[49] Convention of Budapest of 23 November 2001 on cybercrime, *European Treaty Series* No. 185, http://www.conventions.coe.int/Treaty/en/Treaties/Html/185.htm (hereafter: Convention on Cybercrime); Belgium ratified the Convention on 20 August 2012 (date of entry into force: 1 December 2012). See the law of 3 August 2012 on the agreement with the Convention on Cybercrime, done at Budapest on 23 November 2001, *Belgian Official Gazette of* 21 November 2012.

[50] In accordance with Article 1 d of the Convention on Cybercrime, *"traffic data" means any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service."*

[51] If the established principles of the national legal system do not allow this, real-time interception of traffic data and content data must be secured by other means (Articles 20.2 and 21.2 of the Convention on Cybercrime).

[52] Explanatory report to the Convention on Cybercrime of 23 november 2001, http://conventions.coe.int/Treaty/EN/Reports/html/185.htm, § 222 en 230 (hereafter: explanatory report to the Convention on Cybercrime).

[53] However, the Convention on Cybercrime as such does not provide a solid answer to this, in view of the vague wording and the fact that the Convention is only aimed at harmonising minimum competencies relating to investigation in a digital environment (See Article 39 of the Convention on Cybercrime and the Explanatory to the Convention on Cybercrime, §131.) Moreover, it seems that the Convention now for once sets the location of the person obliged to provide cooperation as the criterion to locate investigative actions (see Article 18, a of the Convention on Cybercrime regarding the Production order) and then again the location of the data (see Article 16 in conjunction with Article 29 of the Convention on Cybercrime, regarding the expeditious preservation order). With regard to obtaining subscriber information, suddenly reference is made to the place where an internet service is offered (Article 18 b of the Convention on Cybercrime). Therefore, there are different views to be found in doctrine regarding the location of orders for cooperation. See extensively in this regard: K. DE SCHEPPER, F. VERBRUGGEN, "Can the *Space Invaders* evade our *Pac-Man*? Belgian substantive and procedural criminal jurisdiction in the case of a criminal offence of refusal to cooperate on the part of electronic service providers.", in *B-CCENTRE Report* 2014.

[54] Explanatory report to the Convention on Cybercrime, § 222 and § 230.

[55] Explanatory report to the Convention on Cybercrime, § 222 and 230.

[56] M. GERCKE, *Understanding cybercrime: Phenomena, challenges and legal response*, Genève, International Telecommunication Union (ITU), 2012, 260.

provided regarding the computer system or the telecommunication equipment transmitting the communication. In this way, the Convention combines the subject- and object-oriented approaches to locating real-time investigative acts. When a state intercepts communication at an intermediate station on its territory that is only used for transmitting communication, then, according to the Convention on Cybercrime, such interception occurs on the territory of the intercepting state. The fact that the communicating parties are located somewhere else is irrelevant. This is in sharp contrast to the view in the European Union. Article 20 of the Convention on Mutual Assistance in Criminal Matters provides for the possibility of intercepting communication of persons who are abroad without requiring mutual legal assistance. Although no judicial *assistance* is required, the Article *does* actually require notification to[57] and consent from[58] the state where the persons whose communication is to be intercepted is located. With a view to legal certainty, it is recommended that the location method of the Council of Europe and the location method of the European Union be harmonised.

21. NATIONAL REGULATIONS – As is the case in several other legal systems[59], for instance in Belgium, the legal framework regarding telephone interceptions also apply to interceptions of computer data (art. 90 *ter* Belgian CPC). Consequently, the law of the country where the person is located applies to the interception of his or her communication. This is also evident in Article 90 *ter* §6 of the Belgian Criminal Procedure Code, which outlines the conditions subject to which a foreign authority can apply an interception measure to a person who is located in Belgium, without requiring technical assistance from Belgium. The foreign authority can only use the data that have been obtained by means of such interception on condition that the competent Belgian legal authority agrees with the measure.

B. Towards a uniform locating principle: Focus on the subject

22. SUBJECT: ACCEPTED – Both the Convention on Cybercrime and the EU Convention on Mutual Assistance in Criminal Matters apply a subject-oriented principle: the state on whose territory the subject is located is territorially competent to perform investigative measures in real time in regard to the said subject. This seems logical from the perspective of the principle of sovereignty and the intended legal protection. The sovereign authority of the state where the subject is located (hereafter: subject state) includes the competence of controlling actions performed on and communications conducted from or to its territory. This is subject to the conditions outlined in its national law and the rights and freedoms to which it has committed itself at an international level. In this way, the subject state has control over what happens on its territory. Moreover, a completely subject-oriented approach clearly delineates a territorial border with regard to sovereign competence. When the subject crosses the border, the possibility to unilaterally continue the real-time search also lapses. As a matter of fact, international cooperation is required every time the subject to be intercepted is located abroad, even if no technical assistance is needed from abroad. This approach provides sufficient legal certainty. Legal protection, in particular protection of the right to privacy[60], is provided in accordance with the law of the country in which the legal subject is located, and from where he performs actions and communicates. The state where the subject is located is entitled to exclude other states and can in this way offer its subjects external protection against any foreign interference with their fundamental rights that is unlawful according to national law. Consequently, the interplay outlined above (see no. 4, above) is maintained.

23. SUPPLEMENTED[61] BY OBJECT (CONVENTION ON CYBERCRIME)? – We are of the opinion that it is not advisable to supplement the subject-oriented authority with an object-oriented authority, whereby the location of

[57] If it is known that the person is located on the territory of another Member State before the interception order is given, such notification must be sent before the interception takes place. In other cases, the notification must be made immediately after it has become known that the person is located on the territory of the Member State to be notified.
[58] The investigating state can continue the interception as long as the consent has not yet been given but, in principle, it may not as yet use the data intercepted. See Article 20.4 b. of the EU Convention on Mutual Assistance in Criminal Matters. (See footnote no. 29, above).
[59] See, for example: art. 126 m Dutch Criminal Procedure Code; §100a Strafprozeβordnung (StPo).
[60] Art. 8 ECHR.
[61] An exclusive object-oriented approach would be possibile as well. However, we do not look into this possibility here. Reasons why such an approach is not desirable are comparable to those elaborated in the part concerning virtual remote searches. (see below, no. 34-37.)

the data is per se decisive. In the Convention on Cybercrime, we find a criterion that is based solely on the technical presence of the data. According to this approach, the moment data are technically present on a state's territory, that state can investigate the data in real time in accordance with its national regulations. We are however of the opinion that this technical criterion is wrong. At the very least, the use of this criterion is not formulated as carefully as needed. The investigative method could in fact be used to deliberately search for data relating to communication conducted between persons who are abroad, without any form of international cooperation and without there being a demonstrable link between the data investigated and the investigating state (e.g. by monitoring an Internet Exchange Point[62]). After all, the IT systems (routers) through which the data pass are, to a certain extent, determined randomly.[63] In the situation illustrated in Figure 2, Germany would, theoretically, be able to unilaterally intercept the conversation between Belgian X and Dutch person Y in accordance with German regulations. This hardly seems to be consistent with the sovereignty in its external dimension of the country where the investigated person is located. Even if both communicating parties and the communication service provider are located on its territory, it is possible that other states can access the communication under their national regulations, merely because of the technical construction and operation of the Internet. In this approach, the territoriality plays a limited role. In our opinion, the Internet infrastructure completely erodes the exclusion right of the state where the communication is conducted or virtual actions are performed. As a result, each state loses control of the external legal protection of persons who are located on its territory and who perform actions there or communicate from there. In this way, there is no longer any legal certainty for the legal subjects. We are therefore of the opinion that if a country wishes to intercept data that are by chance present on its territory at a certain moment, state sovereignty and mutual respect between states require more precise rules regarding international cooperation.[64]

2. The search for stored *data*

A. Current object-oriented approach

24. CURRENT PRINCIPLE: LOCATION DATA – When investigating authorities look for physical proof, logically speaking, they do so where the evidence is to be found. If the evidence is to be found abroad, they can only access it by means of international cooperation in line with state sovereignty and the territoriality principle.[65] Consequently, we could state that the remote search for virtual evidence[66], which is stored on an IT system abroad, can also only be obtained by means of international cooperation. This point of

[62] i.e. a type of internet hub to which various services providers' networks are connected and through which they mutually exchange their communication. With regard to the possibility of monitoring an Internet Exchange Point, see: F. BHATTI, J. SOUTER, "ExSERT: Enabling Distributed Monitoring at Internet Exchange Points", 2005, http://saleem.host.cs.st-andrews.ac.uk/publications/2005/lcs2005/lcs2005-hbs2005.pdf; see as well: G.L. HERRERA, "Cyberspace and Sovereignty: Thoughts on Physical Space and Digital Space", 2005, *kms2.isn.ethz.ch, 21-23.*

[63] J. GULDENTOPS, *Geschiedenis en het internet: een historische, methodologische en heuristische benadering van de informatiesnelweg,* Leuven, Acco, 1996, 9; G.L. HERRERA, "Cyberspace and Sovereignty: Thoughts on Physical Space and Digital Space", 2005, *kms2.isn.ethz.ch, 4; See as well: Verslag namens de commissie, Parl. St. Senaat 1999-2000, no. 2-392/3, 22.*

[64] By way of comparison: B. DE SMET, "Registratie en lokalisatie van telecommunicatie" in A. VANDEPLAS, P. ARNOU, S. VAN OVERBEKE, *Strafrecht en strafvordering. Artikelsgewijze commentaar met overzicht van rechtspraak en rechtsleer.,* Mechelen, Kluwer, 2008, 29.

[65] See, for example: European Convention of 20 April 1959 on mutual assistance in criminal matters, *Belgian Official Gazette* 23 October 1975, *err. Belgian Official Gazette* 6 November 1975 (hereafter: CoE Convention on Mutual Assistance in Criminal Matters); Convention of 28 January 1988 between the Kingdom of Belgium and the United States of America on mutual legal assistance in criminal matters, *Belgian Official Gazette* 8 December 1999; EU Convention on mutual legal assistance in ciminal matters; Council Framework Decision of 18 December 2008 on the European evidence warrant for the purpose of obtaining objects, documents and data for use in proceedings in criminal matters, *Pb. L.* 18 December 2008, vol. 350, 72 ff.; Proposal for a Directive of the European Parliament and the Council regarding the European Investigation Order in criminal matters, *CEU* 9145/10, 29 April 2010; F. THOMAS, *Internationale rechtshulp in strafzaken* in *APR,* Deurne, Kluwer, 1998, 290 p.

[66] E.g. the network search, for example (the extension of the search in an IT system to an IT system connected to it, which is located at a distance) or the secret variant thereof, which we like to call the "online investigation". See C. CONINGS, J.J. OERLEMANS, "Van een netwerkzoeking naar online doorzoeking: grenzeloos of grensverleggend", *Computerrecht* 2013, afl. 1, 23-32. In more practical terms, one can think of searching a Dropbox account, an account on social media or a webmail account.

view is not only to be found in doctrine.[67] The Council of Europe and the Belgian national legislator seem to use this as point of departure as well. Article 31 of the Convention on Cybercrime actually deals with mutual legal assistance to access data *stored on the territory of another signatory state.* Article 32 of the Convention on Cybercrime additionally provides for a few exceptions in which it is possible to have direct transborder access (see no. 25, below). The Belgian legislation regarding network search provides a far-reaching unilateral authority, which is not prohibited by the Convention on Cybercrime as such.[68] Article 88 ter §3, paragraph 2 of the Belgian Criminal Procedure Code in fact provides the following: *"If it becomes apparent that these data are not to be found on the territory of the Kingdom, they will only be copied. In that case, the investigating judge communicates this without delay, via the Public Prosecutions Service, to the Ministry of Justice, which notifies the competent authority of the respective State if this state can be reasonably determined."* The preparatory documents explain that, in this way, the legislator wanted to enable the unilateral transborder network search, subject to strict conditions, in order to be able to counter the risk of losing evidence. The legislator adds, however, that if there is enough time[69] and knowledge, the path of the traditional rogatory commission must be followed.[70] Thus, to the Belgian legislator, the location of the data seems to be decisive to determine the location of the investigative measure. He does still however provide a unilateral possibility to perform *transborder searches.* Yet, in a data-oriented point of view, such as the current one of the legislator, this is, in principle, contrary to the prohibition of unilaterally providing for extra-territorial investigative acts.[71]

25. INEFFICIENT CRITERION – As the Belgian pragmatic approach indicates, on a practical level, the current object-oriented approach is confronted with a substantial number of problems. An increasingly larger part of human life is moving to the digital environment. Communication is increasingly taking place through virtual channels such as email, Skype, whatsApp and social media. At the same time, all types of data such as photographs and videos are being stored by using Dropbox or similar cloud services to make it easier to exchange them, secure their sustainability or improve their accessibility. This means that law enforcement agencies, in more and more cases, must search for digital evidence. However, the services that are offered and used through the Internet are not linked to territorial boundaries. Resultantly, investigating authorities are increasingly confronted with the fact that the sought after data are stored abroad. Data are not necessarily located on the territory of the investigating authorities, even if they are linked to a national IT-service. As a consequence, an increasing number of cases are suddenly acquiring an international dimension solely because of the place where the sought after data are stored. International judicial assistance is essential whenever the sought data are located on servers abroad. Therefore, an object-oriented approach requires a disproportional need for international cooperation, which is usually characterised by delays. With such delays, there is always a risk that the volatile evidence may be lost. Further, with the object-oriented approach, states that have many service providers and a large storage capacity are confronted with an overload of requests for legal assistance, which will probably become increasingly difficult for them to process.

Article 32 of the Convention on Cybercrime provides only two limited exceptions for the signatory States. Under the first exception, direct transborder access is possible if the data are accessible to everyone (the internet as open source). This is in line with existing international practice and, consequently, also applies to countries that did not sign the Convention on Cybercrime.[72] The second exception is that direct

---

[67] See: N. SEITZ, "Transborder search: a new perspective in law enforcement?", *Yale Journal of Law and Technology* 2005, Vol. 7, 22 ff; J. SPOENLE, *Discussion paper: Cloud computing and cybercrime investigations: Territoriality vs. the power of disposal?*, Project on Cybercrime Council of Europe, 2010, http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/documents/internationalcooperation/2079_Cloud_Computing_power_disposal_31Aug10a.pdf

[68] Explanatory report to the Convention on Cybercrime, § 294.

[69] In view of the volatile nature of data, the exception is more likely to become the rule, because time will often be lacking.

[70] Memorie van Toelichting, , *Parl. St.* Kamer 1999-2000, 213/1, 24.

[71] PCIJ 7 september 1927, *SS Lotus* (Frankrijk/Turkije)*, C.P.J.I.Rec.* 1927, Serie A, no. 10, consideration 45; See as well on this subject: C. CONINGS, J.J. OERLEMANS, "Van een netwerkzoeking naar online doorzoeking: grenzeloos of grensverleggend", *Computerrecht* 2013, afl. 1, 27 ff.

[72] N. SEITZ, "Transborder search: a new perspective in law enforcement?", *Yale Journal of Law and Technology* 2005, Vol. 7, 38.

transborder access is allowed if a person who has the authority to disclose the sought data grants access to the investigating authorities.[73] This exception only applies within the territorial scope of the Convention on Cybercrime. Therefore, if the location of storage is unknown (see no. 26, below), the investigating authorities cannot know whether the exception applies or not.[74] Further, it is also possible that the data are located in the territory of a state that has not ratified the Convention. And, since this exception requires the specific permission of the person, chances are that the investigating authorities may not succeed in obtaining the required permission in a specific case. Therefore both exceptions contribute little towards solving the problem. This is why vehement debates regarding more far-reaching possibilities for unilateral transborder searches are taking place in the Convention Committee on Cybercrime.[75] In addition, the Convention on Cybercrime is attempting to speed up the cooperation in different ways.[76] However, translating theory into practice is proving to be a laborious task.[77]

26. LOSS OF OBJECT-LOCATION – Lack of time is not the only problem impairing the efficiency of the current system. Lack of knowledge is another serious stumbling block. It is difficult or impossible to pinpoint the precise location of data. Cloud computing is a major contributing factor to this.[78] The "cloud" consists of various servers connected to one another through the internet. Data stored in the cloud are continually moved for financial reasons and in order to render optimum use of the storage capacity.[79] Therefore, locating data at a given moment appears to be practically impossible. Moreover, files in a cloud can be split up into small parts, which can be stored at different locations.[80] In this regard, the Belgian legislator, for example, puts forward a limited solution by enabling a transborder network search when investigators do not reasonably succeed in identifying the state to cooperate with.[81] However, the increasing use of cloud computing is threatening to make the exception the rule. In order to make a criterion for procedural jurisdiction practicable, it is extremely important that investigating authorities can easily estimate in advance how they can apply it in the case they are working on.[82] Furthermore, the criterion may also not be subjected to too much change. That is why the location of data does not seem to be a good criterion.

27. PROVISIONAL POINT OF VIEW? – The Committee of Ministers of the Council of Europe stated in recommendation R(95)13 as far back as 1995 that a unilateral search for data abroad *possibly* entailed

---

[73] This is, for example, a legal user of data being investigated or a services provider who has specified the controlling power in his general terms and conditions. See CYBERCRIME CONVENTION COMMITTEE, "Guidance Note # 3, Transborder access to data (article 32)", 2013, www.coe.int/TCY.

[74] CYBERCRIME CONVENTION COMMITTEE, "Report: Transborder access and jurisdiction: What are the options?", *T-CY* 2012, no. 3, 21.

[75] Zie CYBERCRIME CONVENTION COMMITTEE, "Report: Transborder access and jurisdiction: What are the options?", *T-CY* 2012, no. 3, 69 p.

[76] In this way, Article 25 of the Convention on Cybercrime provides the possibility of using *"expedited means of communication, including fax or e-mail"* to request mutual legal assistance; Article 29 of the Convention on Cybercrime outlines the possibility of requesting a state to order the freezing of data stored by means of an IT system on its territory. Such a request has very few formalities and is used pending a more well-grounded request to provide data (in this regard, see also Article 30 of the Convention); Article 35 of the Convention on Cybercrime provides that 24/7 points of contact be established.

[77] M. GERCKE, *Understanding cybercrime: Phenomena, challenges and legal response*, Genève, International Telecommunication Union (ITU), 2012, 280 (regarding the establishment and use of 24/7 points of contact).

[78] J.J. SCHWERHA, *Law Enforcement Challenges in Transborder Acquisition of Electronic Evidence from "Cloud Computing Providers",* Project on Cybercrime Council of Europe, 2010, http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy_octopus2012/presentations, 9.

[79] B.J. KOOPS, R. LEENES, P. DE HERT, S. OLISLAEGERS, *Misdaad en opsporing in de wolken, knelpunten en kansen van cloud computing voor de Nederlandse opsporing* in *WODC,* Tilburg, Universiteit van Tilburg, 2012, 12; J. SPOENLE, *Discussion paper: Cloud computing and cybercrime investigations: Territoriality vs. the power of disposal?,* Project on Cybercrime Council of Europe, 2010, http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/documents/internationalcooperation/2079_Cloud_Computing_power_disposal_31Aug10a.pdf

[80] B.J. KOOPS, R. LEENES, P. DE HERT, S. OLISLAEGERS, *Misdaad en opsporing in de wolken, knelpunten en kansen van cloud computing voor de Nederlandse opsporing* in *WODC,* Tilburg, Universiteit van Tilburg, 2012, 36.

[81] Memorie van toelichting, *Parl. St.* Kamer 1999-2000, 213/1, 24-25.

[82] J. SPOENLE, *Discussion paper: Cloud computing and cybercrime investigations: Territoriality vs. the power of disposal?,* Project on Cybercrime Council of Europe, 2010, http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/documents/internationalcooperation/2079_Cloud_Computing_power_disposal_31Aug10a.pdf

an infringement of the sovereignty of the country where the data are stored.[83] While the Convention on Cybercrime was being drafted, it seemed that it was impossible to reach consensus regarding the question as to whether or not searching a foreign computer system results in an infringement of sovereignty.[84] Having regard to the extremely limited possibilities for transborder searches under International Public Law, the states found practical agreements for such a search to be essential.[85] Therefore, the Council of Europe did not provide a final answer on the sovereignty issue. In addition, it appears from the explanatory report to the Convention on Cybercrime that its drafters decided only to include in its Article 32 situations that all countries had agreed to. They agreed not to regulate other situations until such time as further experience has been gathered. [86] The Article does not allow far-reaching competencies, but neither does it exclude them.[87] At the time of its adoption, digital investigation was not sufficiently advanced to be able to definitively settle the issue. However, unfortunately, the question regarding the determination of the location of the search, which is closely connected to the issue on sovereignty, was not explicitly mentioned. As is the case for the obligations regarding cooperation (see footnote no. 53, above), hardly any attention is given to the criterion for locating the investigative acts. In this regard, the Convention on Cybercrime labels a search for data stored abroad as a transborder search, without giving much explanation.

28. NEED FOR SUBSTANTIATED CHOICE - The Criminal Procedural locating issue is not explicitly raised anywhere at international level, save in the Convention on Cybercrime and the EU regulations regarding intercepting telecommunication. International Public Law does not offer us any clear solution. However, in our opinion, the traditional logic that the search for physical proof takes place where the evidence is to be found cannot always be extended to a search for digital proof. This logic only applies to direct searches of a computer system (computer search), such as looking into the information stored on a directly accessible computer or a mobile phone. This situation can actually be compared to other searches, such as a search of premises or other places. The place where the proof is to be found and the place where the proof is accessible (to the user and the law enforcement agencies) coincide, which means that the traditional way of locating searches for physical proof can be applied. However, there is an important difference in searches for data stored at a distance, such as a network search, and the online search of an online account (e.g. Dropbox, webmail and social media) (see footnote no. 66, above). The place where the evidence is to be found and the place(s) of access to the evidence no longer coincide. A person can store data across borders but access them and use them where and when he pleases. Consequently, a new situation has arisen, which is not at all comparable to the searches for physical proof in the real world. For this reason, we will consider a few other possibilities to locate remote searches for stored data in order to subsequently compare the current object-oriented point of view with what we regard as the most suitable alternatives.

[83] Recommendation R(95)13 concerning Problems of Criminal Procedure Law connected with Information Technology, http://www.coe.int/t/dghl/standardsetting/media/Doc/CM/Rec%281995%29013_en.asp; see also: MvT, *Parl. St.* Kamer 1999-2000, 213/1, 45-46.

[84] CYBERCRIME CONVENTION COMMITTEE, "Report: Transborder access and jurisdiction: What are the options?"*, T-CY,* 2012, no. 3, 27; H.W.K. KASPERSEN, "Jurisdiction in the Cybercrime Convention", in B.J. KOOPS, S.W. BRENNER (eds.), *Cybercrime and Jurisdiction, A Global Survey*, Den Haag, T.M.C. Asser Press, 2006, 20; See as well: W.H. VON HEINEGG, "Legal implications of Territorial Sovereignty in Cyberspace", in C. CZOSSECK, R. OTTIS, K. ZIOLKOWSKI (eds), *4th International Conference on Cyber Conflict,* Tallinn, NATO CCD COE Publications, 2012, 11-12.

[85] H.W.K. KASPERSEN, "Jurisdiction in the Cybercrime Convention", in B.J. KOOPS, S.W. BRENNER (eds.), *Cybercrime and Jurisdiction, A Global Survey*, Den Haag, T.M.C. Asser Press, 2006, 20.

[86]Explanatory report to the Convention on Cybercrime, § 293.

[87]Explanatory report to the Convention on Cybercrime, § 293.

B. Remote search for stored data territorially reconsidered

a. Possible alternatives

29. LOCATION OF THE INVESTIGATING AUTHORITIES – The first possible criterion to locate the remote search for stored data is the location of the investigating authorities. According to this view, the place where the investigating official is physically located and where he reaches out to the data is also the place where the search takes place. It is only when one physically cross borders, such as to search premises, that international rules on cooperation become essential. However, we find this view far-reaching. An extremely large amount of information, whether encrypted or not, is directly available through the internet. Such information may often relate to foreign matters, persons and objects. To choose the location of investigating authorities as a decisive criterion would therefore clearly cause an impairment of the sovereignty of other states because persons and occurrences on their territory could be cut off from their external legal protection, merely and solely due to a presence in the virtual landscape. Moreover, this view impairs legal subordinates' legal certainty. In this case, they have no idea whatsoever as to when information regarding them, which can be accessed at a distance, can be viewed and controlled by foreign authorities. For example, law enforcement agencies having hacking authorisation at their disposal in accordance with their national law would be able to use this unilaterally to access the secured Dropbox account of a legal subordinate abroad. In our view, the comparison of the computers of the authorities to virtual windows that enable them to perform searches abroad from their own territory is therefore going too far.

30. LOCATION OF THE INVESTIGATED PERSON – We could similarly qualify remote searches for stored data as an investigative act in respect of a person, as is the case in telephone and data interception. Searching for existing digital evidence can be compared to searching for (an aspect of) *someone's* virtual past. The emphasis is then placed on the person being investigated, rather than on the data being searched. In that case, if an investigated person is on national territory, there is no question of an extra-territorial investigation. In this way, each person's legal virtual environment (i.e. all the digital data to which the respective person has remote access, such as online profiles on all types of websites, with the exception of profiles hacked by the respective person (see no. 48, below) is within the spheres of competence of the state on whose territory that person is located.

However, merely extending the application of the locating principle as it applies to real time searches is over-simplifying matters. Searches in real time look at the investigated person's comings and goings at the moment that the search is taking place. By locating such investigative acts in the place where the investigated person is to be found, states are able to control in real time the communication and actions conducted or performed on their territory (see no. 22, above). By contrast, using the location of the investigated person as a criterion to locate the remote search for stored data would imply the following: entering a territory for a holiday, business trip or stopover would make the virtual past of the concerned person, which is stored by means of all types of online accounts, visible to the local authority purely in accordance with national regulations. According to this view, a person would therefore necessarily always take all his digital belongings with him, in so far as these are accessible from a distance, every time he personally transcends the border. Leaving a virtual past at home would then no longer be an option. In our view, this would involve a grave impairment of the free movement of persons and subordinates' self-determination not to submit matters to the direct competence of a foreign authority (see no. 3, above). Having regard to the territorial delineation of sovereignty, an individual exposes himself to the legal competence of a foreign authority every time he transcends the border. His comings and goings fall under the control of the foreign authority, as do the objects he takes with him. If the person does not wish to subject objects, which may contain proof of communication or actions from the past (such as letters, documents, photographs, a laptop or smartphone), to such sovereign authority, then he should not take them along when transcending the border and should leave them at home. We find that depriving persons of such a choice, purely because of the virtual accessibility thereof, displays a lack of subtlety and is undesirable.

31. HABITUAL RESIDENCE – An investigated subject's habitual residence is another possible criterion to determine the location of the remote search for stored data. This approach locates a person's virtual living environment at his habitual residence. It combines the focal point of someone's virtual life with that of his physical life. For example, when law enforcement agencies wish to access a suspect's Dropbox account, there would be no problem in terms of International Law if the suspect's habitual residence is located on the national territory of those law enforcement agencies. Moving one's habitual residence also entails moving one's virtual living environment. A person is assumed to leave his virtual past at home when he physically transcends borders. Having regard to the locating principle in the case of searches in real time, the foreign authority can in fact access the respective person's present-day virtual life (see no. 22 et seq., above), e.g. observing which data the respective person consults during his stay). Furthermore, the foreign authority can unilaterally access the data which the respective person actually takes with him across the border (e.g. data stored on the Smartphone that he carries with him). By contrast, access to the virtual past, independent from the investigated person's simultaneous use of data, such as online search of a Hotmail or Dropbox account or a Google Calendar, is in principle only possible by means of cooperation with the country where the investigated person has his habitual residence (however, see no. 40 et seq., below). As in Tax Law, we could work with presumptions as to the habitual residence of the concerned person.[88] The habitual residence is then presumably the place where the respective person is registered with the national registry. That presumption is refutable, however. In the case of a married or legally cohabiting person, there is an irrefutable presumption that the habitual residence is the place where the family is settled.

32. EXPLANATION: APPLYING THIS TO BELGIUM IN PRACTICAL TERMS – Regulations regarding the various forms of remote searches for stored data could then be along the following lines: If, in the process of investigating a matter, it appears that it is necessary, and less far-reaching measures cannot produce any comparable result, the Public Prosecutor/ Investigating Judge can order a virtual search in respect of a person who [...formulation of further conditions...],[89] and whose habitual residence is on national territory. The search may relate to the entire legal virtual environment relating to the person in respect of whom the investigative act was ordered (see nos. 39 and 48, below). However, the order must also clearly delineate the part of the respective person's virtual living environment that is to be investigated.[90] The approach is valid in respect of public as well as secret virtual searches, on condition that the legislator imposes stricter conditions to the more serious privacy interferences, in accordance with the jurisprudence of the ECHR.[91]

33. LOCATION OF SERVICE PROVIDER CONSULTED – Finally, the investigative act could also be located by means of the location of the service provider through whose services the searched data are stored. Under this approach, it is possible for the United States to examine data on Facebook, irrespective of where Facebook has stored the data searched and the location or nationality of the person to whom such data belongs. This would in any event be more practical than the current criterion because investigation is no longer hindered by the loss of object location (see no. 26, above). Consequently, we also consider this criterion in deciding which main criterion must be taken into account to determine territorial procedural competence.

[88] See art. 2§1, 1° Code of Income Revenu Taxes, *Belgian Official Gazette* 30 juli 1992.
[89] The concrete conditions will depend on the extent of interference with privacy. The following are some of the elements worth to consider in this regard: whether or not the virtual search is secret and the object of the search.
[90] By way of comparison ECHR 3 July 2012, no. 30457/06, Robathin/ Austria.
[91] ECHR 24 April 1990, Kruslin/France , *Publ. Eur. Court. H.R.,* 1990, serie A, no. 176-A; ECHR 25 March 1998, Kopp/Switserland, *Journ. Procès* 1998, no. 347.

b. Comparison

I. EXTERNAL STATE SOVEREIGNTY AND LEGAL PROTECTION[92]

34. OBJECT/SERVICE CRITERION: INFRINGEMENT OF THE SOVEREIGNTY OF THE STATE OF RESIDENCE? - During the preparatory works of the Convention on Cybercrime, it became apparent that it was not clear whether a direct search for data stored abroad constituted an infringement of the sovereignty of the state where the data are stored (hereafter: state of storage) (see no. 27, above). The question whether a more subject-oriented power would therefore infringe the sovereignty of the state of storage remains unanswered. In contrast, the following question does not arise in the preparatory documents, although it is just as important: does the current object-oriented approach not constitute an infringement of the sovereignty of the state where the investigated person is normally to be found (state of residence)? According to the object-oriented approach, the states with the largest storage capacity assume sovereign power over data of persons regardless of where they are located in the world. They further enjoy the right to exclusion in relation to those data. The data constitute a form of externalisation of activities performed on the territory of another state. The place where a virtual life is actually lived is irrelevant in the object-oriented approach. The same applies when the search is to be located in the service provider's state. The state from which the virtual actions are normally performed or the virtual communication is normally conducted (i.e. the state of residence) does not have any competence to autonomously control such actions and communication, apart from real-time search. That state does not have an autonomous access competence to the data, whereas the respective person can consult and use the data on his territory. In order to make control possible, the state of habitual residence would always have to cooperate with the state where the data are stored or the state from which the service is provided. Consequently, it seems to us that, in an object- or service-oriented approach, an infringement of the sovereignty of the state of residence is more likely to occur than an infringement of the sovereignty of the state of storage in a subject-oriented approach. Moreover, the place where the data are stored is most certainly not always the same as the place where the consulted service provider is located. In that case, the object-oriented approach allocates the sovereign competence regarding the data to a state which shows very little connection with the investigated activity or person. In this way, the legal framework is completely alienated from the reality that it aims to regulate. For example, when a Belgian Examining Magistrate wishes to take a look at a resident's Google Calendar during a premises search, he would be required to cooperate with the state on whose territory the Calendar data are stored. Although Google-Inc. is an American company, it does not necessarily store its data in the United States. As a matter of fact, Google-Inc. has various data centres in North and South America, Asia and Europe.[93] They form the *"Google cloud"*, so to speak. The Examining Magistrate would only be able to access the data which is sought under the terms of the national regulations, if they are coincidentally stored in the Belgian data centre. If not, he must procure cooperation from the state of storage. However, to do so, he would first need to know where the data are stored, which is certainly not a simple task.

35. OBJECT CRITERION OF THE CONVENTION ON CYBERCRIME: RIGHT TO EXCLUSION? – In view of the fact that the signatories to the Convention on Cybercrime were of the opinion that a unilateral search for data stored abroad *could* infringe the sovereignty of the storage state, the Convention applies an object-oriented approach. Article 32 of the Convention on Cybercrime provides two possibilities for performing direct transborder searches. Apparently, states reached sufficient consensus regarding the possibility of direct transborder search if the person who has the legal authority to disclose the sought after data consents (Article 32, b of the Convention on Cybercrime).[94] This concerns, for example, the permission a person gives investigating institutions to access his email or other data which he stored across the borders. The

[92] Just as a reminder: In its external dimension, the state sovereignty relates to its (horizontal) inter-functioning with other states. States must recognise one another's sovereignty (external recognition). This enables sovereign equal states to peacefully coexist. The external sovereignty of a state entails a right to exclude other states from the former's own territory, which enables the state to protect its own subjects against unlawful interference by foreign authorities (external protection) (see no. 2, above).

[93] http://www.google.com/about/datacenters/inside/locations/index.html

[94] See CYBERCRIME CONVENTION COMMITTEE, "Guidance Note # 3, Transborder access to data (article 32)", 2013, www.coe.int/TCY. See *supra* no. 27.

ISP can also grant such permission if the contract conditions provide this. Permission by the state of storage is then no longer necessary. Certain private (legal) persons can therefore currently influence sovereignty claims of the state of storage. This is strange because of the fact that national sovereignty does not only guarantee a certain protection to individuals, but it also affects the state's interests.[95] More precisely, an individual is hereby offered the opportunity of overriding the storage state's exclusion right[96]. In this way, an email account owner's permission to the local investigating institutions to access such account sidelines the (possible) interests of the state on whose territory the emails are stored. This seems to indicate, in our opinion, that the signatory states to the Convention are not insisting on the object state's right to exclude the subject state or the service provider's state.

36. SUBJECT CRITERION: INFRINGEMENT OF THE SOVEREIGNTY OF THE STORAGE STATE – In an *exclusively* subject-oriented approach, the state where the subject has his habitual residence would be able to exclude the state where the object is located (i.e. the state of storage). The state of storage may experience the limitation of its competence regarding data that are stored on its territory as an infringement of its sovereignty. Then, in fact, such state no longer has autonomous competencies regarding all objects located on its territory.

II. INTERNAL STATE SOVEREIGNTY AND LEGAL PROTECTION[97]

37. OBJECT/SERVICE CRITERION: CRIMINAL FORUM SHOPPING – Under the current object-oriented approach, authorities can only obtain data stored abroad through the slow international cooperation channels. Criminals can easily abuse this system by shrewdly using cloud services or by storing their data in countries that are known to be difficult in providing international cooperation.[98] To some extent, they can also circumvent the law of their countries by storing illegal content on servers located in countries where such content is not prohibited. Pseudo-child pornography comes to mind here: such material does not involve actual children, and it is not currently punishable in the same way in all countries.[99] Due to the fact that dual criminality can be a determining factor in the willingness of states to offer each other legal assistance, the criminal can manipulate this so as to seriously hamper criminal investigations.[100] In our view, the object-oriented approach in this way prejudices the internal functioning of state sovereignty.[101] One subjects oneself to the competence of a state by entering its territory. The objects the person has in his possession and the actions that he performs on that territory also fall under that authority. He withdraws

[95] M. GERCKE, *Understanding cybercrime: Phenomena, challenges and legal response*, Genève, International Telecommunication Union (ITU), 2012, 277-278.

[96] I.e. the right to exclude other states from one's own territory.

[97] Just as a reminder: In its internal dimension, the state sovereignty relates to its (vertical) inter-functioning with its legal subordinates. State sovereignty can only be maintained if it is supported by sufficient recognition by those who are subjected to it (internal recognition). Such recognition is pursuant to a primary need of order and protection in respect of one's fellow man (internal protection). The state's competence to prescribe and enforce conduct is aimed at satisfying those needs.

[98] G. VACIAGO, "Remote forensics and cloud computing: an Italian and European legal overview", *Digital Evidence and Electronic Signature Law Review,* 2011, vol. 8, 124.

[99] For example, in the United States, virtual child pornography is only punishable to the extent that it cannot be distinguished from real child pornography. See Prosecutorial Remedies and Other Tools to end the Exploitation of Child Pornography Today Act (PROTECT Act), *Pub. L.* No. 108-21, 117 Stat. 650 (2003); M.J. HENZEY, "Going on the offensive: a comprehensive overview of internet child pornography distribution and aggressive legal action", *Appalachian Journal of Law* 2011-12, vol. 11, 23-24. Far-reaching punishment of virtual child pornography has in the past already been labelled as unconstitutional in the United States. See *Ashcroft v. Free Speech Coalition,* 535 U.S. 234 (2002); Art. 383 *bis* of the Belgian Criminal Code, in contrast, makes pseudo-child pornography punishable by using more general terminology: "[...] symbols, objects, films, photographs, slides or other image carriers depicting positions or sexual acts of a pornographic nature, in which minors are involved *or are depicted* […]". Also merely accessing child pornography, without possessing it, is punishable in accordance with Article 383 *bis* § 2 of the Criminal Code.

[100] For example, Article 5 of the CoE Convention on mutual assistance in criminal matters provides: "*Any Contracting Party may […] reserve the right to make the execution of letters rogatory for search or seizure of property dependent on one or more of the following conditions: (a) that the offence motivating the letters rogatory is punishable under both the law of the requesting Party and the law of the requested Party […]* "; see also Art. 14 Council Framework Decision of 18 December 2008 on the European evidence warrant for the purpose of obtaining objects, documents and data for use in proceedings in criminal matters.

[101] See also: P. DE HERT, "Cybercrime and Jurisdiction in Belgium and the Netherlands. Lotus in Cyberspace - Whose Sovereignty Is at Stake?" in X, *Cybercrime and Jurisdiction. A Global Survey,* Den Haag, T.M.C. Asser Press, 2006, 109.

data from the competence of his authority by storing data abroad. For the person concerned, however, such data do, in principle, remain perfectly accessible at any moment in time and from any place whatsoever. Whilst the person enjoys full access and use of that data, he is given the choice to decide whether or not he wishes to withdraw certain objects/information from the state sovereignty of the local authority. This prejudices one of the sovereignty's most important prerequisites, namely internal recognition. Allocating the territorial competence for search exclusively to the state from which the service consulted by the subject is provided would involve a similar problem.

38. SUBJECT CRITERION: RESTORING INTERNAL RECOGNITION – In our view, the subject-oriented approach could restore the balance between the individual and the authority in this regard. Focusing on habitual residence ensures that the most important competencies of control of both the virtual and the physical life are vested in one and the same state. Individuals can no longer escape from the local legal system by storing data abroad, whilst enjoying full access and use of that data. It is only in this manner that the essential internal recognition of the sovereignty of the respective state is restored and that the authority can efficiently fulfil its entrusted task of controlling and protecting.

c. Comparing results

39. STATE OF RESIDENCE: PREFERENCE – It appears from the above comparison that the state where the investigated subject has his habitual residence should be given an autonomous investigative competence with regard to remote search for stored data. The autonomous investigative competence relates to the investigated subject's legal virtual environment. Making this competence dependent on the will of the state of storage or the service provider's state should, in our opinion, be excluded. As is the case with investigations in real time, the focus should be on the subject. However, it is the location of his place of residence, and not his personal location, that is decisive. Moreover, in a subject-oriented approach, legal subjects are given the protection they expect.[102] Regardless of where the data are to be found, the human rights of a person are protected on the basis of the law of the country where he has habitual residence and, in general, where he habitually consults his data. In this way, every virtual action falls within the scope of a coherent and, for the person concerned, familiar system of protection of privacy and other human rights. This also ensures that there is legal certainty.

3. Virtual searches in general: supplementary to the principle criterion?

40. OTHER STATES WITH WELL-FOUNDED LINK – We can conclude from Titles 1 and 2 that the location of the subject and his habitual residence must apply as principle criteria in locating virtual searches. The question still remains whether the competence of the subject state or residential state must be further supplemented by a territorial competence of other states. As is the case with traditional telephone interception, various states may have sovereign competence regarding the same virtual communication or act. In view of the fact that virtual acts display more links with the physical territory than traditional telephone conversations (see no. 14, above), we must verify whether those additional links lead to competencies for the states concerned. In a completely subject-oriented approach (where the focus is on the investigated subject or on his place of residence), no autonomous investigative competence is vested in the state of the service provider consulted by the subject (service provider's state), through whose services the data to be investigated are for example sent or received, (such as Facebook, Yahoo! and Microsoft (Hotmail and Skype)). However, such a foreign service provider does have at its disposal a substantial amount of data, such as traffic and subscribers' data. In contrast to other states, the state where the service provider is to be found does not display a random, technical link (see no. 23, above) but, rather, a well-founded link with these data. This well-founded link can justify a territorial competence on the part of the service provider's state. The same applies to the state where the subject or the service provider consulted by the subject stores his/its data.

[102] See also the following regarding the question on a shifting of the focus from the place where the data are stored to the place where there is an interference in fundamental rights and freedoms: F. CAJANI, *Technologies and Business vs Law - Cloud computing transborder access and data retention*, 2012, 16-17, www.coe.int.

A. Service provider's state

41. SOVEREIGNTY - We are of the opinion that to deny the service provider's state the competence to autonomously investigate the data linked to that service could infringe its sovereignty. If the data sought are accessible to the service provider and are linked to its service, which is consulted by the subject, the service provider's state displays a well-founded link with the data sought and its claim to sovereignty cannot merely be brushed aside. However, data passing through the infrastructure of a service provider do not, in itself, displays a well-founded link with the service provider's state. In our opinion, there must also be clear indications that the service was consulted by the investigated subject and that the sought data are related to the subject's use of the service.

42. LEGAL PROTECTION AND LEGAL CERTAINTY - If a legal subject uses services offered by a foreign service provider, he could also expect that his data can be investigated under the service provider's state's law. By using a service provided from abroad, the legal subject virtually transcends the borders of the territory where he is physically present. The investigated subject is not only physically present in one state, but also virtually enters the territory of another state from where he consults services. He must accept the consequences of transcending borders (see no. 3, above). He personally subjects his data to the sovereign competence of the state (e.g. the United States) from where the service (e.g. Facebook) is provided. Consequently, legal certainty does not present any obstacle for this autonomous investigative competence. We therefore propose that the subject-oriented approach be supplemented with a competence that is based on the place from where the service consulted by the investigated subject is provided. The practical criteria to determine this place must reflect the focus on the subject. Which territory can the subject be presumed to have entered? This must in any event be a place known to the subject.

B. State of storage

43. SOVEREIGNTY - We have already seen that a lack of autonomous competence on the part of the state of storage can constitute an infringement of its sovereignty (see no. 36, above). Here, too, we continue to approach the issue from the perspectives of legal protection and legal certainty. A distinction is needed here regarding to who stores the data abroad.

44. STORAGE BY THE SERVICE PROVIDER - Under the first scenario, the service provider stores data in a foreign country without the express and clear permission or consent of the owner of that data. The state where the service provider stores a subject's data should not be allowed to derive any autonomous competence from such storage with regard to the subject's data. In such a case, matters begin to become distorted at the level of the internal recognition of the territorial limitation of the sovereignty (see no. 3, above). A person must recognise that the sovereignty of his own state is limited and that there are other sovereign states that also have autonomous competencies to be able to fulfil their task of maintaining order and protecting their own territory. Consequently, the legal subject must recognise that when he decides to transcend his own state's borders, he thereby accepts the sovereignty of the state of the territory on which he decides to stay. However, the decision to transcend the borders and to subject himself to a foreign sovereign institution must, in the first place, lie with him personally. If the service provider (e.g. Google) has control over this by storing the legal subordinate's data in a place that is financially more viable, it becomes difficult to the subject to know which state has competence over his data and legal certainty in a virtual environment is therefore eroded. If a legal subordinate chooses only to consult national service providers (e.g. Telenet and Netlog for a Belgian legal subject) so that he does not subject himself to the sovereign competence of a foreign state, the service provider could prejudice that choice by storing the data outside its own national borders. Moreover, the extent of the protection of human rights is then made to fully depend on the place where the service provider chooses to store the data. Cloud computing would only exacerbate this problem, because this involves storing data in different places and constantly moving them around (see no. 26, above). In view of legal certainty and the protection of human rights, the competence of the state of storage must in this case be made to

depend on the cooperation of the subject state / state of habitual residence (depending on the type of investigation) or the state from where the service consulted by the subject is provided.

45. STORAGE BY INVESTIGATED SUBJECT - Under the second scenario, the investigated person himself stores the data in the foreign territory. Every time a legal subject personally stores his data on a specific server across the borders, such storage subsequently involves the competence of the state of storage. This is the case, for example, when a person who has his habitual residence in Belgium, but works in the Netherlands, stores his data remotely on the servers in his office in the Netherlands. In this example, both Belgium and the Netherlands have autonomous investigative competence regarding the data stored in the Netherlands. Belgium has the competencies to perform a virtual search on the grounds of the principle criterion (habitual residence) and the Netherlands has the same competencies on the grounds of the supplementary criterion (the place where the subject stores his data). In all cases, the focus is on the investigated subject and on the question as to whether he transcends virtual borders and thereby subjects himself to the competence of a foreign state. This approach guarantees that the autonomous investigating state always displays a well-founded link with the investigated subject to whom the data relate or to whom they actually belong.

46. NEED FOR AN INTERNATIONAL AGREEMENT - This, however, seems to be an idealistic approach. In practice, it will be difficult, if not impossible, to forbid states, within the scope of a Criminal Law investigation, to access data on their own territory, which, in fact, belong to a legal subject with whom they do not have any clear well-founded link. Moreover, this applies to every state for which the data are technically accessible from its territory.[103] It is only by means of international agreements that countries can effectively restrict one another to a certain extent regarding the possibility of access to data that can be located on their own territory.[104] As long as this does not take place, states can attempt as much as possible to provide protection by restricting the possibilities of their own service providers to perform transborder data storage. Such an approach is currently to be found in the EU Directive on Data Protection.[105] Concerning the transfer of personal data to third countries, the Directive outlines a graduated system, which depends on the protection level offered by the third country regarding the privacy, fundamental rights and freedoms. Where a suitable protection level is lacking,[106] transfer is only allowed under the strict conditions referred to in Article 26 of the Directive. Unconditional agreement by the respective person to whom the personal data relate can then make transfer possible.[107] In the event of such permission, in our perspective, one can also speak of a personal virtual border transcendence by the user of the service. An additional possibility is to shield off domestic data traffic by restricting or excluding intervention by foreign Internet Exchange Points [108] If we wish to counteract such fragmentation of the worldwide internet,[109] we must urgently reach international consensus on how we can restore state sovereignty and the territoriality principle to their original functions.

---

[103] States can indeed indicate that they feel that their sovereignty is infringed when other states investigate data to which they are only technically linked. However, it is doubtful whether this yields any result.

[104] Cf. Art. 20 EU Convention on Mutual Assistance in Criminal Matters.

[105] See Articles 25 and 26 of Directive 95/46/EC of the European Parliament and the Council of 24 October 1995 on the protection of private individuals with regard to the processing of personal data and on the free movement of such data, which somewhat restrict the free choice of storage, *Pb.L.* of 23 November 1995, no. 281, 31-50. See also Articles 40, et seq. Proposal for a Regulation of the European Parliament and of the Council on the protection of private individuals with regard to the processing of personal data and on the free movement of such data (Proposal General Data Protection Regulation), *COM* 2012/0011. See also in this regard US-EU Safe Harbor Framework: http://export.gov/safeharbor/eu/eg_main_018365.asp. ; See for example Russia: http://www.ibls.com/internet_law_news_portal_view.aspx?s=latestnews&id=2609.

[106] The Commission can determine whether or not the protection level is suitable.

[107] See also Article 44 of the Proposal for a General Regulation on Data Protection.

[108] See, for example http://tweakers.net/nieuws/92198/deutsche-telekom-wil-binnenlands-internetverkeer-gaan-afschermen.html

[109] See in this regard "The NSA and the risk to the internet. The US must give Assurances to stop Balkanisation of the web.", *The Financial Times Limites* 2013, http://www.ft.com/intl/cms/s/0/e1643694-4619-11e3-9487-00144feabdc0.html#axzz2kQ1Shqum

4. Cyberspace as virtual territory

47. VIRTUAL TERRITORY - We are of the opinion that we can conclude from the above that the focus on the subject and his virtual transcendence of borders should enjoy preference if we want to maintain territorially delineated sovereignty and the legal protection that is intended by it. This is why we propose that various authorities may have at their disposal autonomous competence to investigate the same virtual data, each on the grounds of a well-founded link between its physical territory and the investigated subject and his data. Consequently, we find that the territoriality principle is still feasible. A symbolic representation can explain what we are proposing. We can take the Internet as what it is: a network of networks,[110] as a *res communis,* like the high seas.[111] Everyone is allowed to use it, but is required to have due regard to the general interests that it serves. However, everything that happens there bears one or more flags.[112] Such a flag is indicative of an adequately well-founded link between the data and the physical territory of a certain state. All data bearing the flag of a certain state jointly form the *virtual territory* of that state. The metaphor of *virtual territory* clearly reflects how we wish to delineate the sovereign competence of a state in cyberspace. Although, at first sight, this wording seems to be a contradiction in terms, it may help to visualise the proposed approach. The virtual territory is an extension of the physical territory and is inextricably linked to it. Consequently, not only does every state have sovereign competencies within its physical territory, but it also has sovereign, albeit often shared, competencies within its virtual territory. In this way, investigative acts performed on a state's virtual territory fall within its territorial spheres of competence. Just as states must recognise one another's sovereignty regarding physical territory, in the same way, they must also recognise one another's sovereignty regarding virtual territory (external recognition). Five elements (cf. five types of virtual flags) determine the virtual territory of a state.

48. HABITUAL RESIDENCE REGARDING VIRTUAL PAST - The changeable borders of the virtual territory are firstly drawn by the competence to access the virtual environment of the persons having habitual residence on the physical territory. Their entire virtual past belongs to the respective state's virtual territory. However, illegal access (e.g. hacking) cannot extend the territorial competence of the respective state due to the fact that this causes illegal entrance in another person's virtual environment. An authority which wants to access this must do so by means of international cooperation with the authority having the sovereign competence over the hacked system. This also applies, for example, to obtaining traffic data, which are stored with a service provider, to which the subject does not have any access. In our view, a national authority to hack the IT system of a foreign service provider in order to thus obtain access to those traffic data is out of the question.

49. LOCATION OF SUBJECT REGARDING VIRTUAL PRESENT - On the other hand, the virtual territory of a state also consists of data related to the virtual real-time activities of persons who can be located on the respective state's physical territory. Those activities can therefore also be intercepted or observed under the conditions referred to in national legislation. Here, too, only the data accessible to the subject are also accessible to the state.

50. LOCATION OF SERVICE PROVIDER – A third component of a state's virtual territory consists of data linked to service providers present in its territory. The state not only has an autonomous investigative competence in respect of its service providers as such, based on the first component of the virtual territory ("habitual residence". Cf. the service provider as investigated subject). The investigating institutions of that state can also unilaterally access data that are linked to the use of the services of the service provider by the investigated subject. It is important that the subject must have consulted the service. The sought data may not be merely passing through the service provider's infrastructure purely for technical reasons. The

---

[110] G.L. HERRERA, "Cyberspace and Sovereignty: Thoughts on Physical Space and Digital Space", 2005, kms2.isn.ethz.ch, 23.

[111] M. HILDEBRANDT, "Extraterritorial jurisdiction to enforce in cyberspace?: Bodin, Schmitt, Grotius in cyberspace", *University of Toronto Law Journal* 2013,vol. 63, 211.

[112] By way of comparison: W.H. VON HEINEGG, "Legal implications of Territorial Sovereignty in Cyberspace", in C. CZOSSECK, R. OTTIS, K. ZIOLKOWSKI (eds.), *4th International Conference on Cyber Conflict,* Tallinn, NATO CCD COE Publications, 2012, 9.

data must be accessible to the service provider. Data regarding an investigated subject, which are accessible only to the service provider, only fall under the sovereign competence of the state from where the services are provided. The subject state or state of habitual residence does not have direct access to this because the subject neither has access to those data.

51. LOCATION OF SUBJECT'S STORAGE – Furthermore, data stored on a state's territory also constitute a part of its virtual territory. However, this is only true for data that the investigated subject stores on the state's territory. It is only in that case that the subject enters the respective state's virtual territory. By contrast, if the data were stored by a service provider that was consulted by the subject (e.g. provider of a cloud service) and the subject did not agree to the particular place where the data are stored, then, only the service provider, and not the subject, enters the respective state's virtual territory. The state then only has access to the data stored on its territory, which directly concern the service provider.

52. INTERNET AS OPEN SOURCE – Finally, data that are accessible to everyone, whether or not this is under restricted conditions, such as registration or payment, also constitute part of the state's virtual territory. There is currently already an international agreement in this regard (see no. 25, above.) There would therefore be almost no change in this respect. According to the new approach, the open part of the internet forms part of every individual's virtual environment. In principle, this part of the internet therefore also forms part of the various states' virtual territory. This part of cyberspace therefore constitutes a prime example of shared territory where different states have autonomous competencies at their disposal.

5. Applicability of the new approach

A. Practical steps forward

53. ACCELERATION OF CRIMINAL INVESTIGATION – At a theoretical level, we have come to the conclusion that a subject-oriented approach to locating investigative acts in cyberspace comes closest to the traditional concept of territorial state sovereignty. Below we examine whether this focus on the subject (and his virtual border transcendence) is also applicable in investigative practice. We have already seen that the current object-oriented approach is particularly problematic because it necessitates a disproportionate reliance on slow international cooperation. The idea of a virtual territory would solve this problem and the criminal investigation could be substantially accelerated. In view of the fleeting nature of digital data, speed is of primary importance to secure proof.

54. COHERENT APPROACH TO THE LOCATING ISSUE – In our opinion, the subject-oriented approach coherently resolves the issue concerning the determination of the location of investigative measures. Traditional investigative competencies always require physical crossing of borders so that they can be performed abroad. However, with regard to criminal investigation, territorial limitation of state sovereignty excludes unilateral physical border crossing by law enforcement agencies. Wiretapping formed the first challenge to thinking in terms of territoriality. The physical crossing of borders was no longer essential to intercept a conversation of a person abroad. It is difficult to determine where the data sought (the communication) are to be found. The national and European legislators did not explicitly address the locating issue but quietly shifted focus from the location of the evidence sought to the location of the investigated subject. In this way, a state only has autonomous competence if the investigated person is on its territory. The Council of Europe later confirmed this approach partly in the Convention on Cybercrime for virtual search in real time. The proposed focus on the subject for virtual searches provides a coherent approach regarding investigation where there is no need to physically cross territorial borders because the evidence is directly available from the investigating state's territory. The location of the investigated person or his habitual residence determines in the first place where the investigative competence is located. What is important in this respect is that the user also does not need to personally transcend the borders to consult the data. This competence must be further supplemented by the competence of the state whose territory the investigated subject enters virtually. There, too, the focus is on the subject. For example, a competence belongs to the state from where the internet services, consulted by the subject, are provided or the state where the subject stores his data. A technical coincidental presence of data (cf.

Article 20 of the EU Convention on Mutual Assistance in Criminal Matters) or transborder storage by a service provider is insufficient to establish investigative competence for the respective state in relation to the data due to the lack of a well-founded link with the investigated subject.

B. Problematic issues

a. Dependence on cooperation of the service providers' state

55. IDENTIFICATION AND DETERMINATION OF LOCATION THROUGH ISP - We take the following situation as our point of departure: The subject to be investigated is suspected of having incited an underage girl to committing indecent acts. To do so, he created a fictitious identity and used an online communication service provided by, for instance, Facebook. If investigating institutions want to perform any kind of virtual search in respect of the suspect, the following must be considered: firstly, the subject-oriented principle vests sovereign competence in the state where the investigated subject (in this case, the suspect) is to be found or where his habitual residence is located (in this case, both unknown). That competence is supplemented by the sovereign competence of the state from where the service consulted by the subject (in this case, Facebook) is provided (in this case, the United States). The digital environment often makes it extremely difficult to locate the individual behind the virtual action or communication in the physical world. In this regard, Internet Service Providers (ISP) and Internet Access Providers (IAP) are an important source of assistance for investigation institutions.[113] In principle, ISPs (in this case: Facebook) can check which IP address accessed their services at which moment in time (if they store such data). In the example, Facebook could check which IP address was used to connect to the investigated fictitious profile at the moment at which the illicit sexual acts were incited. The IP address shows which IAP (e.g. Belgacom or Telenet) granted access to the internet and, therefore, from which country the action or communication took place.[114] In its turn, the IAP can provide more concrete information on the identity of the person using its services (e.g. the number of the modem consulted or the subscriber's particulars).[115] It is therefore extremely important that the obtaining of their cooperation for location and identification takes place as efficiently as possible. This can be problematic in an international context. The service providers will often be foreign nationals. There are diverse views on the question as to whether enforcing a national legal obligation to cooperate on a foreign-national service provider is in accordance with International Law.[116] It therefore seems to us that it is advisable to cooperate with the state where the service provider is to be found. However, the investigation then strongly depends on the extent to which the state from where the services consulted by the subject are provided is prepared to cooperate. In principle, as long as investigating institutions do not know whether the investigated person is to be found on the territory of the investigating state or has his habitual residence there at the time of the investigation, no virtual searches can be performed autonomously regarding the suspect. In the first place, it will therefore need to find out where the investigated person is to be found or where he has his habitual residence.

56. LACK OF COOPERATION - However, over-dependence on the cooperation of the state where the service provider is to be found is problematic. The investigation may become deadlocked when there is no cooperation. This enables the criminal to make use of services that are provided from states that are

[113] C. CONINGS, P. VAN LINTHOUT, "Sociale media: een nieuwe uitdaging voor politie en justitie.", *Panopticon* 2012, afl. 3, 208-209.
[114] For Belgium, see, for example: http://www.nirsoft.net/countryip/be.html. Depending on the circumstances, these data can contain serious indications of the location of the subject or his habitual residence.
[115] C. CONINGS, P. VAN LINTHOUT, "Sociale media: een nieuwe uitdaging voor politie en justitie.", *Panopticon* 2012, afl. 3, 208-209.
[116] See P. DE HERT, G. BOULET, "De Yahoo-saga: de keuze tussen nationale tracingsmethoden en internationale rechtshulpinstrumenten", *Computerr.* 2012, afl. 5, 324-330; K. DE SCHEPPER, "Medewerking in een virtuele context? Ya! Hoo echter afdwingen?", *AM* 2012, afl. 2-3, 239-243; K. DE SCHEPPER, F. VERBRUGGEN, "Can the *Space Invaders* evade our *Pac-Man*? Belgian substantive and procedural criminal jurisdiction in the case of a criminal offence of refusal to cooperate on the part of electronic service providers.", in *B-CCENTRE Report* 2014; J. VANDENDRIESSCHE, "The effect of 'virtual presence' in Belgium on the duty to cooperate with criminal investigations: some prudence may be required when confronted with a request from a Belgian public prosecutor", *DEASLR* 2011, afl. 8, 194; with regard to vagueness in this respect, see the Convention on Cybercrime: footnote no. 53, above.

known to be difficult in providing international cooperation. In this way a criminal can personally contribute to the obstruction of a local criminal investigation. Resultantly, internal recognition of the sovereignty, which constitutes a substantial prerequisite for such sovereignty, is eroded (cf. no. 37, above). This problem can be solved only when the service provider's state is prepared to come to certain agreements. When the location or habitual residence of the investigated person is unknown, investigating institutions will feel compelled, in cases of anonymity and lack of international judicial assistance, to assume competence as subject state or state of residence.[117] As soon as there are serious indications at hand that the subject is to be found in a third state or has his habitual residence there (depending on the type of investigation), international rules regarding cooperation will be required once again.

57. SLOW COOPERATION – When the state of the service provider is indeed prepared to cooperate, such cooperation often takes too long. This is why efforts must be made to accelerate international cooperation in investigating a virtual environment. The already existing possibility of requesting a freezing order can offer a solution. However, in our opinion such request should be addressed to the state where the service provider is established.[118] When the requested state discovers that a service provider from a third state or from the requesting state was also consulted regarding the data sought (e.g. IAP (Telenet)), that state can immediately communicate the necessary traffic data to the requesting state so that the latter can be afforded the opportunity of securing all the data sought from all the service providers involved.[119] Both forms of cooperation can be refused when (1) the crime leading to the request for judicial assistance constitutes a political crime or is linked to such a crime, or (2) the requested state regards the freezing or communication as being contrary to its sovereignty, security, public order or other essential interests. However, it would be more efficient if service providers were to be directly approachable. The protection of human rights may however not be made subordinate to the efficiency of the criminal investigation. Yet, in our view, it should be possible and is advisable to impose on states by means of a Convention on Cybercrime II the obligation to instruct their ISPs to directly answer to certain orders by certain foreign authorities.

58. DIRECT COOPERATION BETWEEN CONSTITUTIONAL STATES – Possible direct orders could firstly concern location. The ISP would be able to indicate to which country the IP address used refers without communicating the IP address as such. When it becomes apparent that the investigated subject acts on the territory of the investigating state or when the ISP has information that indicates that the investigated subject has his habitual residence on the territory of the investigating state, the ISP's direct approachability could be maintained. They could then directly communicate the IP address or assist the respective authority in its search for data. A direct freezing order could also be issued pending a more well-founded request to provide data. The states concluding the Convention would have to designate a national institution that could be authorised to directly address the ISPs. The other signatory states to the Convention would be notified of such a decision. In this way, abuse through a lack op authority can be avoided. However, we are of the opinion that direct responses to such requests for information must be subjected to the requesting state's respect for fundamental rights. The Council of Europe could draw up a list of countries

[117] As long as the investigating institutions do not know which state is the subject or residence state, it will not be known whose sovereignty is infringed. In our opinion, such an assumption of competence is also necessary when both the place from where the services are provided and the place where the investigated person is to be found or where he has his habitual residence is unknown. Example: an investigation into a criminal service provider through which a suspect establishes an illegal trading business. In our opinion, if only the place from where the service is provided is unknown, a state could also assume competence as a service provider's state if the cooperation of a state that has the competence on the grounds of another criterion is unworkable. In all cases, the investigation must firstly be aimed at determining the unknown factors.

[118] Cf. Article 29 of the Convention on Cybercrime, which provides the possibility of addressing a request for judicial assistance, requiring few formalities, to the state of storage for the freezing of the sought data, pending a more well-founded request to provide the data sought. (Explanatory report to the Convention on Cybercrime, no. 283). We are of the opinion that it is difficult to make a request to the state of storage practicable. As a matter of fact, investigating institutions will usually need the service provider's technical assistance to freeze data. Moreover, the state of storage is often unknown or the service provider's assistance is required to identify such state of storage. It therefore seems to us that a request to the state where the service provider is established is necessary.

[119] By way of comparison: Art. 30 Covention on Cybercrime.

which satisfy this requirement.[120] With regard to the parties to the ECHR or equivalent legal instrument (in respect of both the content and the control system),[121] a refutable assumption of respect for fundamental rights could apply. This could be an important incentive for states to provide efficient legal protection. Furthermore, a standard form could be provided that must be used by the designated investigating institutions in the requesting states to make their request, in which *inter alia* the suspected crime, the reason why the person is suspected and the necessity for the search should be indicated. The required information would be more limited for the freezing order than for the order to provide data.[122]

59. SUBSIDIARITY PRINCIPLE – Good accessibility on the part of an ISP is more important than it may seem on first sight. The subsidiarity principle, according to which the least drastic measure appropriate for the intended purpose has preference is, in our view, inherent to a system effectively protecting fundamental rights[123] Having regard to this principle, preference should be given to direct consultation of the ISP or to international cooperation above, for example, a national competence to hack into computer systems[124] (e.g. mailbox of a subject having his habitual residence in the investigating state) if the same result can be achieved in this manner. However, that preference only applies if the direct consultation or international cooperation also works effectively. If direct access (such as hacking) is the only way to attain a satisfactory result, the investigating state shall feel compelled to use that competence if the conditions in accordance with the national law are satisfied.

b. Loss of subject-location

60. ANONIMISING TOOLS – Anonimising tools pose an additional problem. Even if investigating institutions succeed in procuring the necessary IP address by means of the cooperation of an ISP, it is still not certain whether they can actually locate and identify the investigated subject. All types of publically available tools, such as proxy servers[125] or The Onion Router (TOR)[126]in fact enable internet users to conceal their identity. It is then difficult, if not impossible, to trace not only the identity, but also the location of the respective person. Investigating institutions will therefore only be able to continue to operate in cooperation with the country where the service provider consulted by the investigated subject is to be found or the country where the subject is seemingly (but not actually) to be found.

61. SERIOUS SIGNS OF ANONIMISING TOOL - In any event, we argue that states must be able to act unilaterally if there are serious indications that the subject is using anonimising tools. This should only be possible if the

---

[120] By way of comparison: art. 25 and 26 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. See also art. 40 proposal General Data Protection Regulation.
[121] By way of comparison ECHR 30 June 2005, no. 45036/98, Bosphorus/Ireland, no. 155.
[122] With regard to the freezing order: art. 29, 2 Convention on Cybercrime.
[123] See in the framework of art. 8 ECHR: P. DE HERT, *Art. 8 EVRM en het Belgische recht,* Gent, Mys & Breesch, 1998, 42.
[124] With regard to hacking competence, see: Dutch legislative proposal to amend the Criminal Code and the Criminal Procedure Code on improving and reinforcing the tracing and prosecution of computer criminality (Act on computer criminality III), http://www.rijksoverheid.nl/documenten-en-publicaties/kamerstukken/2013/05/02/wetsvoorstel-aanpak-computercriminaliteit.html. National hacking competence can also present problems, however, if the state where the hacked system is to be found regards this as criminal access to the computer system. See C. CONINGS, J.J. OERLEMANS, "Van een netwerkzoeking naar online doorzoeking: grenzeloos of grensverleggend", *Computerrecht* 2013, afl. 1, 30.) This problem arises because of the difference between the proposed locating principles in Criminal Procedure and the current locating principles in substantial Criminal Law (see footnote no. 17, above). However, the reciprocity principal can lead to states tolerating such action. Clear international agreements are advisable, however.
[125] See, for example www.proxy4free.com. By using a proxy offered here, a user can create the impression that he is accessing the internet from a country other than the country where he is in fact to be found. Various users exchange IP addresses through such websites.
[126] The TOR network uses the Onion Routing technique. This technique repeatedly encrypts a message and sends it from the sender to the receiver via so-called onion routers. Each onion router removes an encryption layer and in this way learns to which subsequent router the message must be sent. These intermediaries conceal in this way the origin, destination and content of the message. This makes it practically impossible for investigating institutions to reconstruct the path between sender and receiver. The message leaves the TOR network by means of an exit node and reaches the desired final destination. Investigative institutions can only see the IP address of the exit node. Therefore, keeping an exit node entails a substantial number of risks. See D. GOLDSCHLAG, M. REED, P. SYVERSON, *Onion Routing for Anonymous and Private Internet Connections,* Communications of the ACM, February 1999, vol.42 No. 2, 39-41; See also the article "HTG explains: Is Tor really Anonymous and Secure*",* http.//www.howtogeek.com.

cooperation of the state of the service provider consulted by the investigated subject cannot provide a solution. It will not be possible to know which sovereignty is infringed by the continued performance of the investigation as long as the investigating institutions do not know which state is the state of residence or the subject state. That is why investigating institutions should be able to assume competence. However, they should make every effort to firstly discover the location of the subject or his place of residence (depending on the type of investigation). As soon as there are serious indications that the subject is to be found on the territory of a third state or has his habitual residence there, said state's sovereignty must be respected and its cooperation must be obtained to continue the investigation or the investigation must be continued by that state. Making any other assessment would profoundly disrupt the balance between individuals and the state. In this way the individual would in fact have too much power to hinder a criminal investigation.

C. Summary

62. DETERMINING COMPETENCE: HOW THIS WOULD WORK IN PRACTICE – The diagram below helps to determine whether, based on our proposal, a state's investigating institutions are territorially competent and, therefore, can conduct a criminal investigation in accordance with their national laws. It also indicates when it must/can obtain cooperation from another state, and what that state may be. Some explanation is necessary here:

The questions in the diagram must always be answered on the basis of *serious indications* (reasonable cause).

- Definitions:
    - The subject is the (legal) person in respect of (which) whom the investigative act is performed. This is not necessarily the suspect.
    - The notion "data" always refers to the data sought by the investigating institutions.
    - The service provider (SP) must always be a SP that is consulted by the subject. Merely transmitting data through the SP's channels is insufficient.
    - The concept "accessible" refers to legal access.
- All options must always be pursued. State X, Y and Z must be identifiable states. As long as this is not the case, the answer to the question is "unknown". *Therefore, there may be various final solutions* (e.g. various possibilities for cooperation).
- If, after having pursued the various possibilities, "competent" is reached, one can unilaterally start searching for the data for which purpose the diagram was applied.
- If one of the possibilities is "assuming competence", all other results must first be considered. Competence can only be assumed if these other results are not practicable (e.g. cooperation). When competence is assumed on the basis of an unknown factor, the investigation must primarily be aimed at identifying the unknown factor. The diagram must be gone through again as soon as there are serious indications that allow the unknown factor to be filled in.
- When there are serious indications that anonimising tools are being used, the questions can also be answered as they seemingly appear to be, in addition to the option provided.

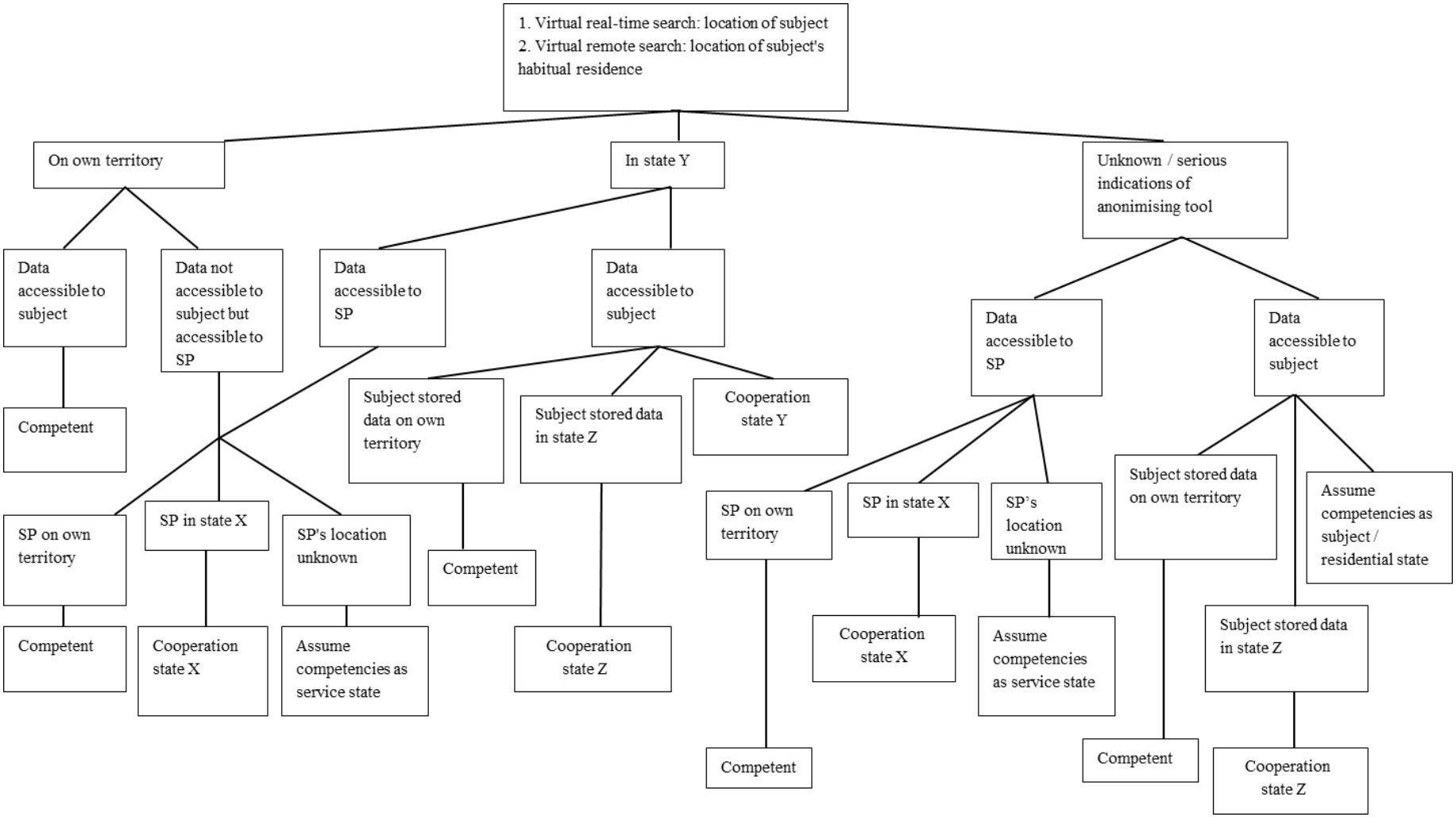


Figure 3: Diagram of territorial competence/need for cooperation for virtual search.

Conclusion

The territorial limitation of state sovereignty restricts the competence of investigating institutions to their own territories. The question regarding how we must locate investigative acts territorially has not yet been explicitly and unequivocally answered in international and national law. The place where the investigative acts take place is often self-evident. However, it is more difficult to answer that question when the location of the sought evidence is unclear or the place where the evidence is to be found is not the same as the place of access to the evidence. Digitisation of the world and, therefore, also of possible evidence, presents us with serious challenges.

If we want to sustain the territorially limited sovereignty and the legal protection intended by it, then we must put the focus on the investigated subject in order to locate virtual investigative acts. That approach is particularly innovative for searches relating to data stored at a distance. In this regard, national and international legislators (provisionally) opt for a focus on the place where the sought data are stored. However, we are of the opinion that this focus is based on a logical error. The object-oriented approach, with which we are currently working, is a further development of the locating principle applied to searches for physical evidence. However, this approach may not and cannot be blindly applied to the virtual remote search. Not only does the object-oriented approach infringe the sovereignty of the state where the data are being consulted by the subject, it also undermines the interaction between legal protection, state sovereignty and territoriality, which is fundamental to our legal way of thinking. Moreover, the current approach appears to be unworkable in practice.

We are of the opinion that the subject-oriented approach is imperative to secure state sovereignty, legal certainty and protection of fundamental freedoms and human rights. Focusing on the subject also benefits the efficiency of the criminal investigation, although this entails particular problems that states will be required to face primarily by means of practical international agreements. Depending on the type of investigation, the place where the subject is to be found or the place where he has his habitual residence determines competence. In addition, the investigated subject's virtual crossing of borders also entails competence. Such crossing is involved when the investigated subject consults foreign services or stores data on particular servers abroad. The extremely large need for legal assistance is in this way replaced by direct access for investigative institutions to their sovereign state's virtual territory. However, one question still remains unanswered: Are we finally ready for thinking in terms of virtuality in our legal system?

Belgian substantive and formal criminal jurisdiction in the case of prosecution of foreign electronic service providers for failure to cooperate.

Can Alien Space Invaders evade the Belgian Pac-Man?[1]

De Schepper, K. and Verbruggen, F.

"*Everyone imposes his own system as far as his army can reach.*" (J. STALIN)

I. The Weak Bite of Belgian Pac-Men?

1. CYBERSPACE: THE FINAL FRONTIER? - "*Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. On behalf of the future I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather.*" This is how internet activist John Perry Barlow begins his "Declaration of the Independence of Cyberspace".[2] This quote, reminiscent of *Star Trek,* gets to the core of the problem with which we are confronted nowadays: how can our traditional legal standards be transposed into the new digital world? For instance, how do we locate behaviour in a world where the dimensions of time, space and movement are blurring? More specifically, how do we construe the concept of jurisdiction in cyberspace? The (Belgian[3]) *Yahoo* case forces us to seek an answer to this question. The Belgian prosecution service initiated criminal prosecution of a US dotcom for failure to respond to production orders (or requests, *infra*) for user identification data issued by a Belgian prosecutor. The prosecution is based on the assumption that American company Yahoo! Inc. (hereinafter "Yahoo") fell under Belgian territorial jurisdiction and therefore no mutual legal assistance from the US authorities is required.

2. IS THE BARK WORSE THAN THE BITE? - Everyone agrees that this *Yahoo* case is a clash of principle. It revolves around the territorial scope of a duty imposed upon private operators to cooperate with law enforcement authorities during a criminal investigation. The Belgian Criminal Procedure Code (Belgian CPC) imposes a duty to disclose the identity of the user of an ICT-application to law enforcement, when ordered to do so by a prosecutor or judge. Failure to comply is punishable with a criminal fine. But how does, or how should, Belgium exercise this enforcement mechanism in a cross-border IT context? And who exactly is to be punished? This has enormous practical importance, and not just in criminal investigations. The increased electronic communication tools available to the public, create a corresponding need for investigators to obtain rapid access to information related to such communication. It is also of importance to the interrelation of substantive criminal law (creation of certain offences) with procedural criminal law (the legal obligation to cooperate with a criminal investigation). This interrelation complicates the answer to the difficult question of which State can claim jurisdiction over the internet, its players and its users. Traditionally, international public law, which regulates or limits the jurisdictional claims of individual States, has appeared less opposed to an extensive application by States of their substantive criminal law ("substantive criminal jurisdiction"), as long as they do not effectively press these criminal jurisdiction claims home through the cross-border coercive law enforcement measures or through cross-border imposition of criminal law sanctions ("formal criminal jurisdiction").[4] Do the criteria of international law, which originate from the real world of physical national borders, still apply in the "virtual world" of the internet?

3. COOPERATION ORDER. - Criminal investigation is the organised gathering of information with a view to establish offences, to identify their perpetrators and to find evidence. It is thus a specific, targeted and

[1] Note that "Pakkeman" is Antwerp slang for police or 'cops', when used as a kind of bogeyman.
[2] John Perry Barlow co-founded the Electronic Frontier Foundation (EFF), an NGO that fights for free digital citizen rights and against State intervention in the internet ("cyberlibertarianism"). See https://projects.eff.org/~barlow/Declaration-Final.html.
[3] Not to be confused with the French *Yahoo* case on the offer of French prohibited Nazi memorabilia over the Internet (Tribunal de Grande Instance Paris (Superior Court in Paris), 22 May 2000, *UEJF and Licra/Yahoo! Inc. and Yahoo France*, http://www.juriscom.net/txt/jurisfr/cti/tgiparis20000522.htm).
[4] Permanent Court of International Justice (PCIJ), 7 September 1927, *SS Lotus* (France/Turkey), *PCIJ Collection of Judgements* 1927, Series A, no. 10, 19; International Court of Justice, 14 February 2002, Case concerning the arrest warrant of 11 April 2000 (Democratic Republic Congo/Belgium), International Court of Justice Reports 2002, 3; C. RYNGAERT, *Jurisdiction in International Law*, Oxford, Oxford University Press, 2008, 23.

proportional collection of information. Typically, in the course of a criminal investigation, i.e. an exercise of State power, investigators can obtain, by compulsion, information which the holder does not want to disclose. Orders can be used in addition to requests. These days, much of the information which is of interest to the criminal investigation is not held by the government, but by private entities with relevant technical knowhow and access to the information. This is why the Belgian parliament established in article 46 *bis* Belgian CPC the possibility to an order cooperation. Under such an order, an operator of an electronic communication network or a provider of an electronic communication service is compelled to cooperate in identifying 'the habitual user' of the service or the 'subscriber'. Anyone who refuses or offers inadequate cooperation faces a criminal fine from 26 to 10,000 euros.

Art.46*bis*-orders should help investigators to link telephone numbers, email-addresses and IP addresses to specific users. Indeed, the internet offers users more possibilities to protect their real identity than many other channels of communication do. Such a protection is not always a bad thing. It preserves privacy and freedom of speech. People are more likely, for example, to post their controversial or unpopular opinions on forums if they can do so without disclosing their identities. Anonymity also protects people from unwanted or unwarranted control by public or private entities, from screening of social networking sites by marketing companies, from fraudsters and would-be intruders and from censorship by authoritarian regimes.

In cyberspace, therefore, anonymity is a means to safeguard freedom of speech, as well as privacy and private communication. But neither of these two fundamental rights is an absolute one. In some situations and under some conditions, states may intervene (Article 8.2 and 10.2 of the European Convention of Human Rights [ECHR]). This is definitely justified to detect crime, to collect evidence or to identify and prosecute the perpetrators. States can therefore, within the limits set by their national legislations and by the texts protecting fundamental rights and freedoms, uncover the identity of criminal suspects on the internet. Indeed, the European Court of Human Rights (ECtHR) has condemned Finland for prioritising an internet user's privacy over the rights of a child that had been the victim of "an abuse of identity".[5] The order to produce user data under article 46*bis* Belgian CPC therefore offers investigators a means to find perpetrators or to gather evidence.

Needless to say, this is not a purely Belgian problem. Information on the internet is immaterial, volatile, and processed and stored across national borders. One State's detection and prosecution of crime might very well clash with another State's sovereignty. The search for a compromise to stop the World Wide Web from becoming (or remaining?) a World Wild West is well underway. This Yahoo (test) case, which has turned into an exciting legal saga, certainly helps steer a course.[6]

II. *Pac-Man* versus the *Space Invaders*

1. The cause: "virtual" availability and presence

4. PREVIOUSLY ON… [7] - The Public Prosecutor in the Belgian town of Dendermonde established that Yahoo email addresses had been used in an attempt to defraud a Belgian company. These email addresses

[5] ECHR, 2 December 2008, *K.U./Finland*, no. 2872/02. This was a case of abuse of identity. Someone had created a false profile on a social networking site for an existing 12 year old, and had contacted others in a sexually enticing way. Under the Finnish legislation of the time, "representing oneself falsely as someone else" was not an offence that allowed the government to force internet companies to disclose the identity of the user. Therefore, the ECHR found that Finland had failed in its positive duty under Article 8 ECHR to protect the victim's private life.

[6] This Article contains an analysis of the various judgements to date in the sensational case against Yahoo. At the time of editing, the case was pending before the Antwerp Court of Appeal after the Court of Cassation had quashed the decision for a second time.

[7] For the exact facts, see the original request issued by the Prosecutor, cited as part of the judgement. See Criminal Court of Dendermonde, 2 March 2009, *Tijdschrift voor strafrecht* (*T. Strafr.*) 2009, issue 2, 117-120. See also P. DE HERT and G. BOULET, "De Yahoo-saga: de keuze tussen nationale opsporingsmethoden en internationale rechtshulpinstrumenten", *Computerrecht* 2012, issue 5, 324-330; P. DE HERT and G. BOULET, "Yahoo! moet meewerken met Belgische prosecutor", *De Juristenkrant* 2012, issue 253, 8; K. DE SCHEPPER, "Medewerking in een virtuele context? *Ya!Hoo* echter afdwingen?", *Auteurs en media* 2012, issue 2-3, 239-243; N. VANDEZANDE "Yahoo! als operator of verstrekker", *Auteurs en media* 2011, issue 2, 220-223; L. KERZMANN, "L'affaire Yahoo! ou à qui s' adresse l'obligation de collaboration instaurée par l'Article 46*bis* du Code d'instruction criminelle?", *Revue du Droit des Technologies de l'Informatique* 2011, issue 44, 116-123; J. VAN DENDRIESSCHE, "The effect of 'virtual presence' in Belgium on the duty to cooperate with criminal investigations: some prudence may be required when confronted with a request from a Belgian public prosecutor", *Digital Evidence and Electronic Signature Law Review* 2011, issue 8, 194; P. VAN LINTHOUT, "Yahoo is

were the only link to the perpetrators, but consisted, as they so often do, of false names or non-identifiable pseudonyms.
Therefore, the Public Prosecutor decided to order Yahoo, on the basis of Article 46 *bis* Belgian CPC, to disclose the identification and registration details of the users, including the IP addresses used when the email accounts were set up.[8]
The Prosecutor noted that the Yahoo portal site listed several email addresses and URLs for users to report abuse or to ask questions about security. He took this to be a sign that Yahoo "*is present on Belgian territory, being reachable and available in Belgium*".[9] He then sent his request to these digital contact points. The company subsequently responded by asking that the request be sent to its registered office (in California). The Public Prosecutor sent his request to that address by fax and ordinary post. Yahoo answered that the data were subject to the laws of the United States of America and that it could only disclose the information if asked to do so by an *American* judicial authority. In response, the Public Prosecutor summoned the company to appear before the Belgian criminal court. He based the summons on a breach of the duty to cooperate set out in Article 46 *bis*, §2 Belgian CPC. The Prosecutor argued that Yahoo offers its services in Belgium, over the internet and, as a consequence, the company may not be present in Belgium *physically*, but it is present *virtually*, and hence subject to the Belgian duty to cooperate. In sum, the Prosecutor was seeking the required cooperation from a "*US subject encountered and operating in Belgium, albeit virtually*".[10] Yahoo was therefore obliged to carry out the prosecutor's order to provide the data and hand them over to the authorities in Belgium. In sum, anyone who "is present" in Belgium (be it only 'virtually') is required to comply with a Belgian prosecutor's orders to produce data, even if this entails "going home to America to retrieve them".[11]

2. Twists and turns of a protracted legal battle

5. DENDERMONDE: "VIRTUAL" PRESENCE. - The criminal court of first instance judged that the duty to cooperate applies to any operator/ISP who is present on Belgian territory in a physical or virtual sense and who provides services in Belgium.[12] If this operator/ISP is economically present and available to the Belgian consumer, it is also present and available from a legal point of view. As a consequence, the Public Prosecutor had merely requested "*something in Belgium from a US subject encountered in Belgium where it does business and provides services*". The latter must abide by the laws of Belgium, as does anyone else who "is in Belgium".
The Dendermonde court found that in the case at hand a request for international legal assistance was unnecessary because the order related to a disclosure of information relating to the registration of electronic traffic on *Belgian territory*. According to the court, a request only had to be made through international legal assistance channels, if it related to the transfer or seizure in the US of data with no territorial link to Belgium and if the holder of that data was not present in Belgium ("*neither physically nor virtually*"). In sum, the Public Prosecutor's view prevailed.

6. GHENT APPEAL: NOT A PROVIDER, BUT A USER. - The court of appeal in Ghent took a different view. It found that the cooperation duty did not apply to Yahoo, because the company was not the provider of an electronic communication service.[13] In the court of appeal's view, Yahoo does not provide a service that

---

geen verstrekker van elektronische communicatie", *De Juristenkrant* 2010, issue 216, 4-5, *err.*, *De Juristenkrant* 2010, issue 217, 9; F. VAN LEEUW, "Criminalité informatique: entre objectif et objection d'ubiquité. Quelques pistes de la procedure pénale belge face aux acteurs du 'Cyberworld'" in *Convegno di Studi*, *OLAF*, Bruylant, 2010, 391-418.

[8] An IP address is the number of a computer that is used to log into the internet. Every computer has a unique IP address and is identifiable by it. Comparable to a telephone number or, better still, a unique, numbered "token" that grants (temporary) access, but can be issued to successive users. When someone creates a false email account, he or she uses an IP address, by which it is possible to trace him or her.

[9] The prosecutor equates accessibility by users who are in Belgium with presence in Belgium. We do not think this is right, *see infra* no 17.

[10] Quote from the case report (procès-verbal), from the Dendermonde judgement. See Criminal Court of Dendermonde, 2 March 2009, *T. Strafr.* 2009, issue 2, 119.

[11] In this, he rests on two Court of Cassation judgements on the compulsory identification of registration plates in road traffic offences (see *infra*, no. 31): Court of Cassation, 27 April 2010, P.09.1625.N, *Pasicrisie Belge* 2010, issue 4, 1283; *Nullum Crimen* 2011, issue 6 , 371 note V. FRANSSEN and S. VAN DYCK; Court of Cassation, 22 April 2008, P.08.0250.N, *Pasicrisie Belge* 2008, issue 4, 986; *Rechtskundig weekblad* 2008-09, issue 33, 1383 note P. ARNOU; *Verkeer, aansprakelijkheid, verzekering* 2008, issue 5, 463; *Nullum Crimen* 2009, issue 2, 123.

[12] Criminal Court of Dendermonde, 2 March 2009, *De Juristenkrant* 2009 (report by E. DE BUSSER), issue 186, 3, *T. Strafr.* 2009, issue 2, 116, note.

[13] Ghent, 30 June 2010, *Computerrecht* (NL) 2010, issue 6, 351, *De Juristenkrant* 2010 (report by P. VAN LINTHOUT), issue 216, 4, *T. Strafr.* 2011, issue 2, 132, note P. VAN LINTHOUT.

consists of the whole or partial transmission of signals via electronic communication networks (Article 2, 5° of the Act on Electronic Communication (ECA)[14]). [15]
Yahoo's webmail system is located in American territory and is available via the different internet networks. However, Yahoo itself does not play a part in the transmission of data from Belgium to Yahoo's portal site. That site is only accessible through the intervention of Belgian network operators and electronic communication service providers. They make it possible for internet users to consult the American website from Belgium ("*i.e. made virtually visible on a screen in Belgium*") and are therefore responsible for transmitting the electronic communication. Yahoo merely uses the existing infrastructure and communication services. It is not, therefore, the provider of an electronic communication service, but is itself a user of these services and networks.[16] Nor does this sort of "virtual visibility" allow the suggestion that Yahoo might be present in Belgium in another way and transact business here under the scope of Article 46 *bis* Belgian CPC. The court therefore thought that despite its "virtual visibility" in Belgium, Yahoo did not have the legal status required to fall within the *ratione personae* scope of the co-operation offence in Article 46 *bis*, §2 Belgian CPC.
The court merely looked at whether the defendant satisfied one of the subjective requirements of Article 46 *bis*, §2 Belgian CPC. Having answered in the negative, it remained silent about the geographical ambit of the Belgian rules in cross-border situations (application *ratione loci*).[17] The prosecutor appealed to the Court of Cassation because he found that this narrow interpretation was a breach of Article 46 *bis* Belgian CPC and the general legal principle of the autonomy of criminal law.

7. FIRST QUASHING: BOTH USER AND PROVIDER. - The Court of Cassation quashed the Ghent court's judgement in early 2011.[18] It judged that the duty to cooperate applies to anyone who offers electronic communication services, regardless of whether they are a *Belgian operator in the sense of the ECA*. Also, anyone who enables one's customers to receive, obtain or disseminate information through an electronic network can be a provider of an electronic communication service. The Court of Cassation therefore viewed Article 46 *bis* Belgian CPC as applicable not only to companies that administrate networks and/or provide routing services, but to anyone who offers a service that allows an information exchange via an electronic communication network. It follows then that Yahoo is not merely a user, but a *provider* of electronic communication services, at least in the sense of Article 46 *bis* Belgian CPC.
The judgement was ground-breaking because the Court of Cassation interpreted the law in plain contrast with the intention expressed by Parliament in the preparatory works (*see infra*, no. 20 et seq.). However, the Court of Cassation's review was limited to issues addressed by the contested Ghent judgement. Since the Ghent court did not cover the jurisdiction issues, the Court of Cassation did not elaborate on that subject either. It quashed the Ghent acquittal and send the case to the Court of Appeal in Brussels for retrial.[19]

---

[14] Act of 13 June 2005 on electronic communication, *Belgian Official Journal* 20 June 2005 (hereinafter "ECA").
[15] For example Belgacom, Telenet, Scarlet, Evonet, Toledo Telecom, edpnet, etc. See the statement of Solicitor General De Swaef, *Nullum Crimen* 2011, issue 1, 79 et seq. (specifically no. 10); N. VANDEZANDE, "Yahoo! als operator of verstrekker", *Auteurs en media* 2011, issue 2, 222.
[16] Comparable with classic mail. Yahoo supplies mail addresses only, in a manner of speaking, and makes post boxes available, but does not provide delivery or courier services. In other words, it does not carry the mail. For that, it has to make use of postal services.
[17] This we deduce from the Court of Cassation judgement of 18 January 2011. The Court of Cassation stated that the appeal judges had not accounted for the jurisdiction of Belgian courts of law in their assessment of the personal operating sphere. Nonetheless, we wonder whether the appeal judges should first decide this question before moving on to the personal operating sphere. In other words, by addressing whether the Belgian offence related to the person at hand, it had implicitly decided that Belgian criminal law did indeed apply to the situation at hand.
[18] Court of Cassation, 18 January 2011, General Cause List P.10.1347.N, *Auteurs en media* 2011, issue 2, 218, note N. VANDEZANDE, *Nullum Crimen* 2011, issue 1, 76, statement De Swaef, *Revue du Droit des Technologies de l'Informatique* 2011, issue 44, 113, note L. KERZMANN, *T. Strafr.* 2011, issue 2, 120, note P. VAN LINTHOUT.
[19] The principle is full reversal, the exception limited reversal. The quashing relates to the non-differentiated operative provisions of the contested judgement. The parties can, within the limits of that quashing, use all of the arguments they brought before the first judge. However, the court of a different geographical area of Belgium to whom a case is send upon quashing cannot deny it has jurisdiction over the case sent to it by the Court of Cassation (Articles 23 and 139 of Belgian CPC). Logically, this rule departs from the general (internal legal) procedural rules of territorial jurisdiction. This would not, in our opinion, apply to the rules of jurisdiction as a result of the territorial operating sphere of Belgian criminal procedure, which is assessed on the basis of Article 3 and Article 4 Belgian CC in conjunction with Articles 6 to 12 *bis* of the First Title of the Belgian CPC. In other words, the court that receives a case from the Court of Cassation can still decide that it does not have jurisdiction on the grounds of Article 3 or Article 4 of the Belgian Criminal Code in conjunction with 6 to 12 *bis* of the First Title of the Belgian CPC. The (internal) jurisdiction rules describing the sphere of competence of the different Belgian courts are not mentioned in the latter. See Court of Cassation, 8 October 1986, *Court of Cassation judgement* 1986-87, 162, no. 72; R. DECLERCQ, *Beginselen van strafrechtspleging*, Mechelen, Kluwer, 2010, 659 and 1734-1736; T. DECAIGNY, "De territoriale bevoegdheid na cassatie", *T. Strafr.* 2007, issue 4, 264;

8. BRUSSELS APPEAL: NO PROCEDURAL JURISDICTION. - The Brussels Court of Appeal acquitted Yahoo with a reasoning condensed in a mere five sentences. It stated that, as a matter of principle, a Belgian prosecutor had no power to investigate outside of the Belgian territory.[20] According to the court, Yahoo had not been faced on the Belgian territory with a valid request in the sense of Article 46 *bis*, §2 Belgian CPC . The fact that Yahoo is virtually present in Belgium makes no difference. "*The mere fact that it is technically possible, for parties such as the Public Prosecutor, to reach the defendant from Belgian territory by electronic or other means of communication does not constitute sufficient grounds to issue a valid request*." Even though the Brussels court did not state it in so many words, one can infer from its judgement that the prosecutor should have sought international legal assistance from the US.[21]
The judgement dismissed the position of the Dendermonde court of first instance quite radically. The latter had found that virtual presence and availability of services to Belgian residents were a sufficient territorial link to justify the jurisdiction of the Belgian State. The appeal judges, on the contrary, drew an implicit distinction between *substantive* and *procedural* jurisdiction. Since they decided on the merits of the case, they evidently had did not question their own jurisdiction on the basis of Article 3 of the Belgian Criminal Code (Belgian CC). This means they qualified the facts of the case as a Belgian territorial[22] offence (*see infra*, no. 17). They made it clear, however, that the Belgian prosecutor had no procedural jurisdiction to issue an order to produce the data to the foreign company. And so, between the lines of the decision, we can read that a constitutive element of the offense was missing (i.e. the existence of a valid request in the sense of Article 46 *bis*, §2 Belgian CPC).

9. SECOND QUASHING: NOT AN INVALID REQUEST. - The Public Prosecutor lodged a new appeal to the Court of Cassation, which pronounced itself once more on the case on 4 September 2012. The prosecutor had contested the Brussels Appeal court's view that there was no evidence "*of a valid request by the Public Prosecutor in the territory of Belgium obliging the defendant to disclose information within the meaning of Article 46* bis, *§2 of the Criminal Procedure Code*". He argued that the Brussels court misrepresented the legal value of the document in the case file which contained the request. The judgement was also said to violate Article 46 *bis* Belgian CPC because the request in the case file satisfied the formal and substantial requirements of the law. The way in which the request was sent abroad did not affect its legality.
The Court of Cassation quashed the appeal judgement on this point and cryptically held: "*The circumstance that the Public Prosecutor send his written request, under Article 46* bis *of the Criminal Procedure Code, by which cooperation was requested from an electronic communications network operator or electronic communications service provider based outside the territory of Belgium, from Belgium to an address in a foreign country, does not invalidate that request*[23]." The Brussels Appeals court had given insufficient reasons to vindicate its conclusion that Yahoo had not breached the duty to cooperate.[24]
The case is now pending before yet another Court of Appeal (Antwerp) and thus the question concerning substantive jurisdiction has not yet received a final answer.[25] In our opinion, the Court of Cassation judgement did not contain a definitive ruling as to the scope of the Belgian procedural jurisdiction.[26] It did not state on whether the request entails a binding obligation to cooperate on someone who is located outside Belgium; or, to put it another way, whether the request gives rise to a criminal, punishable duty to cooperate on the part of Yahoo, whether it is actually an *order* to them (*see infra*, no. 27 et seq.). The Court of Appeal in Antwerp will have to clarify this point.

10. LEGAL ISSUES. - What makes the *Yahoo* case so fascinating is how each of the parties has its own vision on the role of the internet in the establishment of jurisdiction, more particularly with regard to the electronic communication services provided by Yahoo and their availability over the internet. According

R. DECLERCQ, "De rechtsmacht van de straf rechter na cassatie", *recent Court of Cassation judgement* 2000, 255; G. STESSENS, "Locus delicti van drughandel", *Rechtskundig weekblad* 1998-99, 1254.
[20] Brussels, 12 October 2011, *Auteurs en media* 2012, issue 2-3, 238, note K. DE SCHEPPER.
[21] See also E. DE BUSSER, "Yahoo weigert IP-adressen door te spelen aan Belgisch gerecht", *De Juristenkrant* 2009, issue 186, 3.
[22] Because if they had considered it to be an extraterritorial offence, they would have had no jurisdiction in the absence of an explicit legal provision establishing such jurisdiction (Article 4 Belgian CC in conjunction with Article 6 to 12 *bis* of the First Title of the CPC).
[23] This is our own underlining.
[24] Note that with this, the Court of Cassation says nothing about the actual (in)validity of the request in question. The Court leaves it in the middle.
[25] See *supra*, footnote 19.
[26] See in this sense, too, O. LEROUX, "Arnaques, frauds et escroqueries sur internet: moyens concrets d'investigation. Point sur l'affaire Yahoo! à la suite du second arrêt de la Cour de cassation", *Journal des tribunaux* 2012, 842.

to the prosecutor, Yahoo has a duty to cooperate with him because it provides services in Belgium over the internet. He terms this as a "virtual" presence in Belgium, from which he then deduces a "virtual" availability of Yahoo data to the Belgian authorities: the duty to cooperate can be located in Belgium, therefore Yahoo is obliged to disclose the information. The Public Prosecutor frames the situation in strictly territorial terms: Yahoo is present and available in Belgium over the internet. Hence, the request a handover of data from a US subject present in Belgium. Yahoo, stresses the extraterritorial feature of the situation: the US corporation is not based in Belgium and therefore does not have a duty to cooperate with Belgian authorities. The request was sent to the US, where a Belgian prosecutor lacks authority. Yahoo's position is that the prosecutor has requested something in the US from a US subject who is based there.

We believe that the answer lies somewhere between both positions. The Yahoo-case is complex, as we have said, because it intertwines issues of substantive and procedural criminal jurisdiction. Indeed, Belgium enforces the criminal procedure duty to cooperate by rendering failure to oblige a criminal offence (albeit one punished with a fine). On top of that, there is the issue of the geographical scope *ratione personae*, i.e. the question of whether foreign providers of webmail are also subject to this duty. We believe that the confusion of substantive and procedural criminal jurisdiction flows from the incorrect use of "virtual" presence by the prosecutor to establish that the duty to cooperate existed and that the offense was committed in Belgium. As a result, it seems that the both parties have at times lost sight of the basic principles of substantive and procedural jurisdiction.

The criminal behaviour is insufficient cooperation or complete absence of cooperation, i.e. a punishable "failure to act", a punishable *omission*. The exact location of an omission is harder to determine than that of a physical *action*, precisely because that which was supposed to happen *did not*. This is why Belgian jurisprudence and legal doctrine '*geolocate'* offences of omission at the location where a person should have fulfilled the duty to act. One must first determine *who* was under the duty and *where* this person had to comply with that duty.[27] These two matters relate to *criminal liability* for the Belgian punishable duty to cooperate (substantive criminal jurisdiction *ratione personae* and *ratione loci*). But we should add that between the questions of *who* and *where*, there is third question that has not as yet received adequate consideration in the Yahoo-case: at *what point* does that duty to act come into being? We would say that the answer depends on *where the person on whom the duty rests is located* (in Belgium or abroad) and on *how that duty comes about in a trans-border context*. This relates to the trans-border *enforcement* or *compulsory execution* of this duty of cooperation (procedural criminal jurisdiction *ratione loci*).
In our opinion, the internet does play a role in this case, in justifying a foreign company's *liability* for a Belgian failure to cooperate which punishable with a criminal fine (broad interpretation of substantive jurisdiction, see chapter 3). On the other hand, in our opinion, this would not (yet?) lead to direct *enforceability* of this Belgian procedural obligation. We think that extraterritorial addressees are not obliged to comply with a request sent to them by a Belgian prosecutor, unless their own authorities endorse this request (narrow interpretation of procedural jurisdiction, see chapter 4).

III. Location of offenses and their perpetrators on Belgian territory

1. The territoriality principle as ground for criminal jurisdiction

11. FORMS OF JURISDICTION. - It is not easy to define the concept of legal authority or jurisdiction. The term originates from the Latin *ius dicere*, or the right to lay down the law. Jurisdiction is historically inseparable from the concept of sovereignty.[28] Through his prerogatives (*imperium*), the sovereign imposed his will and laws on his subjects. The sovereignty was expressed by the promulgation of laws, by their application and by the adoption of measures to ensure that these laws are obeyed and court decisions were respected. We might therefore define jurisdiction as the power to affect people's legal interest either through legislation, through an enforceable order or a court decision.[29]

[27] This also makes the *Yahoo* case particularly difficult: the duty to act rests with a foreign company and not a natural person and it is difficult to determine whether the company is "present" in a given territory or not.
[28] A. CASSESE, *International Criminal Law*, New York, Oxford University Press, 2008, 49.
[29] C. RYNGAERT, *Jurisdiction in International Law*, Oxford, Oxford University Press, 2008, 5 and especially footnote 15.

This definition gives rise to three distinct forms of jurisdiction.[30] The first is *jurisdiction to prescribe*, or the power to issue general laws. This relates to the (geographical) scope of criminal law. Subsequently, *jurisdiction to adjudicate* is the power to judge legal subjects and to subject them to the powers of legal institutions which enforce the law in a specific case. According to Article 3 Belgian CC, jurisdiction resides with the Belgian criminal courts when a crime is committed within the Belgian territory. Any exception to this principle, i.e. extraterritorial jurisdiction, must be set out by the law (Article 4 Belgian CC in conjunction with Articles 6 to 14 of the Preliminary Title of the Belgian CPC). Finally, *jurisdiction to enforce* means the right to ensure that the behavioural norms it issued can indeed be enforced through the use of public force. This means that a Belgian judgement can have cross border effects (e.g. confiscation of a property located abroad). Where there is no extraterritorial jurisdiction to enforce, Belgium will have to rely on the jurisdiction of foreign authorities. Below, we will confine ourselves to jurisdiction to prescribe and jurisdiction to adjudicate. The principles of jurisdiction to enforce are covered in chapter 4.

12. TERRITORIALITY PRINCIPLE. - Territoriality is one of the four bases for jurisdiction recognised under international law, and undeniably the most obvious.[31] If a State is to claim jurisdiction over a crime, there must be an objective link between the State and the crime.[32] The territoriality principle assigns jurisdiction (to adjudicate) to the State in which the crime, or an element of it, was committed.
The territoriality principle also grants a state the power to render behaviour criminal if it physically takes place within its territorial borders, regardless of whether the victim is in the country or not. Belgium can, for example, criminalise fraud or the laundering on its territory of money illegally gained outside of Belgium. For offences consisting of illegal *actions*, the focus lies on where the action begun.[33] It also allows a state to criminalise acts when the *consequences* of those acts are felt within its territorial borders, even if the perpetrator is acting from abroad.[34] A territorial crime can, in other words, have an extraterritorial perpetrator. Here, jurisdiction is claimed because the goal or the result of the criminal behaviour is situated on the territory. The transfer of illegal money to a Belgian account using internet banking, for example, will be punishable under the Belgian law on money laundering, even if the money launderer was sitting behind a computer screen outside of the Belgian territory.

13. RATIONALE. - Territoriality is the most traditional criterion of jurisdiction and still the prime basis for criminal jurisdiction under international law. The reason for this is also symbolic: whenever its laws have been broken, the State has to reassert its sovereignty.[35] It wishes to signal that it does not tolerate reprehensible acts on its territory and that it will protect its citizens and the rule of (its) law. Enforcement of the laws confirms the authority of the State (a matter of legitimacy) and acts as a deterrent.[36] The territoriality principle is also a logical choice from the viewpoint of legal certainty for individuals: we can expect the people of a given country to know and abide by its laws. On the other hand, the courts of the state in which the crime took place may be best placed to see it in its correct context. The territoriality principle also has a practical slant. The locus of perpetration is often also the place where the evidence and perpetrator can be found (*forum conveniens*).[37] Finally, many States try, if possible, to avoid the potential

---

[30] See Restatement (Third) of US Foreign Relations Law (1987), §401; C. RYNGAERT, *Jurisdiction in International Law*, Oxford, Oxford University Press, 2008, 9; B.J. KOOPS and S.W. BRENNER, "Cybercrime jurisdiction–an introduction" in *Cybercrime and Jurisdiction. A Global Survey*, The Hague, T.M.C. Asser Press, 2006, 3.

[31] Other (extraterritorial) grounds are: 1) the personality principle: this considers the nationality of the perpetrator (active personality principle) and the nationality of the victim (passive personality principle); 2) the protective principle: a State may demand jurisdiction if its national interests have come under threat as the result of a crime; 3) the universality principle: it is accepted that a State can claim jurisdiction over a number of crimes recognised by the international community as being of universal importance.

[32] R. AUGUST, "International cyber-jurisdiction: a comparative analysis", *American Business Law Journal* 2002, 534.

[33] In English legal doctrine this rather confusingly termed as "the subjective variant of the territorial principle" because this is the place where the perpetrator was at the time of the act. M. HIRST, *Jurisdiction and the ambit of the criminal law*, New York, Oxford University Press, 2003, 113; V. LOWE and C. STAKER, "Jurisdiction" in M.D. EVANS (ed.), *International Law*, New York, Oxford University Press, 2010, 321-322. See also T. VANDER BEKEN, *Forumkeuze in het internationaal strafrecht. Verdeling van misdrijven met aanknopingspunten in verschillende staten*, Antwerp-Apeldoorn, Maklu, 1999, 50.

[34] The same legal commentary calls this "the objective variant", T. VANDER BEKEN, *Forumkeuze in het internationaal strafrecht. Verdeling van misdrijven met aanknopingspunten in verschillende staten*, Antwerp-Apeldoorn, Maklu, 1999, 50. See also C. RYNGAERT, *Jurisdiction in International Law*, Oxford, Oxford University Press, 2008, 30 and 76.

[35] Y. CARTUYVELS, "Justitie en genocide: bedenkingen voor een discussie", *Orde van de dag* 2002, issue 17, 8; T. VANDER BEKEN, *Forumkeuze in het internationaal strafrecht. Verdeling van misdrijven met aanknopingspunten in verschillende staten*, Antwerp-Apeldoorn, Maklu, 1999, 41.

[36] A. CASSESE, *International Criminal Law*, New York, Oxford University Press, 2008,336.

[37] A. CASSESE, *International Criminal Law*, New York, Oxford University Press, 2008, 451; P. DE HERT, "Cybercrime and Jurisdiction in Belgium and the Netherlands. Lotus in Cyberspace - Whose Sovereignty is at Stake?" in *Cybercrime and Jurisdiction. A Global Survey*, The Hague, T.M.C. Asser Press, 2006, 93.

legal complications of extraterritorial jurisdiction. International law compels States to respect each other's sovereignty and forbids them from intervening in each other's sovereign affairs.[38] In this sense, territoriality is a consequence of the sovereign equality of States. Going beyond their own borders often implies a violation of the sovereignty of other States, which does little to foster peaceful coexistence. Extra-territorial jurisdiction can lead to intervention in the legal system of another country, to a potential clash with the legislation of the territorially competent State and to positive conflicts of jurisdiction, where several countries claim jurisdiction.

14. FROM 'UNI-TERRITORIAL' TO PARTLY TERRITORIAL. - The original logic underpinning the territoriality principle was that crime was a local phenomenon and had to be handled locally.[39] The territory in which the perpetrators had committed the crime had the strongest link with the crime and therefore took preference. This viewpoint slowly eroded over the years.[40]
In 1935, several members of the Harvard Law School made a study of the grounds for criminal jurisdiction.[41] One of their observations, already in those days, was that crime, as the result of improved travel and communications, was no longer a local phenomenon. They therefore accepted that a State could claim territorial jurisdiction over multi-territorial acts, if some *aspect* could be located in *their own territory*. The concept of territoriality is therefore gradually expanded as the basis for criminal jurisdiction.[42] It also allows States to regulate extraterritorial acts with territorial effects (*supra*, no. 12). As we will see below, this expanded concept of territoriality can result in problems, especially in the context of the internet.[43]

15. OBJECTIVE UBIQUITY. - The Belgian theory of objective ubiquity is an example of this type of application of the expanded territoriality principle to multi-territorial acts.[44] If a criminal offence is committed on the territories of several States (multi-territorial crime), Belgium will have jurisdiction if one of the objective elements (parts of the *actus reus* or other objective elements of the offence) of an offence as defined by Belgium, can be located in Belgium.[45] The effect or the result of the offence will only lead to territorial jurisdiction if that effect is also a constitutive element of the crime (a *constitutive* effect). This will, of course, depend on the specific provisions of the criminal statute. The classic example is a murder, since the death of the victim is a constitutive element of the crime. On the other hand, the discharge of waste into a French river, leading to harmful effects in Belgium, is not a Belgian environmental offence because the effects are not part of the definition elements of offence. The environmental offence is an inchoate offence which focuses on the risk generated by the illegal disposal of waste and it is thus immaterial whether (and where) the consequences of the illegal discharge are felt.[46]

Belgian courts also claim territorial jurisdiction when they find that an offence committed abroad and one located in Belgium are *indivisible*.[47] They consider themselves competent (read: they assume they have jurisdiction) with regard to foreign participants to a Belgian crime or when foreign criminal acts form an indivisible unity with criminal acts committed in Belgium. They use typical continental dogmatic constructions like a "continuous" and - less obviously[48] "continued offence" to link extraterritorial events

[38] A.M. SACHVEDA, "International jurisdiction in cyberspace: a comparative perspective", *Computer and Telecommunications Law Review* 2007, 246.
[39] R. AUGUST, "International cyber-jurisdiction: a comparative analysis", *American Business Law Journal* 2002, 536.
[40] T. VANDER BEKEN, *Forumkeuze in het internationaal strafrecht. Verdeling van misdrijven met aanknopingspunten in verschillende staten*, Antwerp-Apeldoorn, Maklu, 1999, 362 et seq.
[41] HARVARD LAW SCHOOL, *Research in International Law: II. Jurisdiction with respect to crime*, *American Journal of International Law* 1935, 435; see R. AUGUST, "International cyber-jurisdiction: a comparative analysis", *American Business Law Journal* 2002, 536.
[42] Y. CARTUYVELS, "Justitie en genocide: bedenkingen voor een discussie", *Orde van de dag* 2002, issue 17, 8.
[43] P.L. BELLIA, "Chasing Bits across Borders", *The University of Chicago Legal Forum* 2001, 65-70 and the interesting discussion in the American literature between the supporters of "cyberlibertarianism" and those of "cyber-conservatism" on whether the internet can be regulated. See, among others, J.L. GOLDSMITH, "Against Cyberanarchy" in *University of Chicago. The law school. Occasional papers*, Chicago, University of Chicago. Law school, 1999, 40, p. 1-37; D.R. JOHNSON and D.G. POST, "Law and Borders - The Rise of Law in Cyberspace", *Stanford Law Review* 1995-96, issue 48, 1367-1402; L. LESSIG, "The Zones of Cyberspace", *Stanford Law Review* 1995-96, issue 48, 1403-1411.
[44] Other location theories are: 1) the doctrine of physical action, being the place where the action physically took place, 2) the doctrine of the instrument, i.e. the place where the instrument had its effect, and 3) the doctrine of effect, where a crime is located where the effects were felt.
[45] Court of Cassation, 7 June 2011, P.11.0172.N., *Nullum Crimen* 2012, 68, note S. DEWULF. The Court uses this doctrine when interpreting "committed on the territory of the Kingdom (…)" in Article 3 Belgian CC.
[46] Article 16.6.2 of the Decree of 5 April 1995 on general provisions of environmental policy, *Belgian Official Journal* 3 June 1995; C. VAN DEN WYNGAERT, *Strafrecht, Strafprocesrecht en Internationaal Strafrecht in hoofdlijnen*, Antwerp, Maklu, 2006, 1210.
[47] Court of Cassation, 24 January 2001, *Revue de droit pénal* 2001, 721.
[48] A continued offence contains a series of criminal acts which relate to the same perpetrator through a unity of objective (unity of purpose). The doctrine of continuing crime, however, relates to the sentencing rules (Article 65

to Belgium. They claim territorial jurisdiction when an inseparable aspect or element of a crime is manifest within the territory of Belgium, even if this relates to effects that manifest themselves after the criminal act is committed, but that form an indivisible whole with them nonetheless.[49] STESSENS calls this "concealed" extraterritorial applications of Belgian criminal law.[50] Belgian criminal law is applied to acts committed abroad under the veil of a territorial application of criminal law. Therefore, its ambit *ratione loci* stretches beyond the territory of Belgium and some acts are treated as if they were committed in Belgium while they actually were not.

The combination of objective ubiquity theory with the doctrine of indivisibility in Belgian jurisprudence can lead to an application as a matter of fact of what is known as the 'effects' doctrine.[51] Here, the criminal court takes account not only of the constitutive effects of the crime, but the further removed effects. A classic example was the so-called the *Teheran cheque* judgement of 1979.[52] In 2008, the criminal court of Dendermonde applied this doctrine in a (domestic) cybercrime case.[53] The perpetrator was prosecuted for the offences of computer forgery (Article 210 *bis* Belgian CC) and hacking (Article 550 *bis*, §1 and §3, 3° Belgian CC). He had hacked a Hotmail account and changed the logins, so that the victim was no longer able to access his account. The perpetrator also had gained access to accounts on various job websites, where he had changed the victim's profile. The court in Dendermonde established its jurisdiction on the basis of the indivisibility doctrine. It found that the place where the victim had noticed that he was no longer able to login and that his profile had been changed were jurisdictional aspects that formed an indivisible whole with the crime.

This case demonstrates that a *de facto* application of the effects doctrine in cybercrime cases can give the criminal court an extremely broad competence. The question arises whether such a development is actually desirable. The ubiquitous nature of the internet means that the effects of cybercrime can be felt anywhere, often *across borders*. Too wide an application of the effects doctrine can therefore have the same detrimental consequences as extraterritorial jurisdiction; the very consequences that States seek to avoid by prioritising the territoriality principle, such as legal uncertainty and conflicts of legislation (see *supra*, no. 13).[54] The place where the effect was felt often also depends on purely coincidental circumstances. For example, had the victim checked his email while on holiday in New York, would it be a court in New York that had jurisdiction? We might, for that matter, ask ourselves whether the judge went a step too far in this case. This is because the effects doctrine requires that the effect can be qualified as a constitutive element of the offence.[55] Noticing that your email account has been hacked hardly qualifies as one of the *actus reus* elements of hacking.[56] In our opinion, the court would have done better

---

Belgian CC). To assess the issue of guilt and therefore, by definition, the jurisdiction check, criminal acts may only be connected. This raises the question of whether that connection can give Belgian courts jurisdiction over acts committed abroad. See J.J. HAUS, *Principes généraux du droit pénal belge*, 1879, I, 249. See also the statement of Advocate General R. Declercq in the Court of Cassation, 16 May 1989, *Court of Cassation judgement* 1988-89, p. 1079. Use of the criterion of (unity of) purpose is also inconsistent with the scope of objective ubiquity theory. This is because only an *actus reus* can be used as a territorial condition in Belgium. B. SPRIET, "(Extra)territoriale werking van de Belgische strafwet" in BELGISCH-LUXEMBURGSE UNIE VOOR STRAFRECHT (ed.), *Strafprocesrecht en extraterritorialiteit*, Bruges, die Keure, 2002, 8 et seq.

[49] Consider, for example, aggravating circumstances.

[50] G. STESSENS, "Locus delicti van drughandel", *Rechtskundig weekblad* 1998-99, 1252.

[51] P. VAN LINTHOUT, "Territoriale bevoegdheid in cyberspace", *T. Strafr.* 2009, issue 2, 113. C. VAN DEN WYNGAERT, *Strafrecht, Strafprocesrecht en Internationaal Strafrecht in hoofdlijnen*, Antwerp, Maklu, 2006, 1212; T. VANDER BEKEN, *Forumkeuze in het internationaal strafrecht. Verdeling van misdrijven met aanknopingspunten in verschillende staten*, Antwerp-Apeldoorn, Maklu, 1999, 55.

[52] Court of Cassation, 23 January 1979, *Court of Cassation judgement* 1978-79, 575. In this case, it was decided that the issue of a cheque without covering funds can be located in Belgium if it is drawn against a Belgian bank. However, the offence is committed at the time of issue, so that drawing a cheque cannot be a constituent element of that offence. C. VAN DEN WYNGAERT, *Strafrecht, Strafprocesrecht en Internationaal Strafrecht in hoofdlijnen*, Antwerp, Maklu, 2006, 1212: J.P. SPREUTELS, "Escroquerie, cheque sans provision et competence territoriale", *Revue de droit pénal* 1981, 237-258.

[53] Criminal Court of Dendermonde, 29 September 2008, *T. Strafr.* 2009, 111-112, note P. VAN LINTHOUT. According to the internal rules of procedure on jurisdiction (Articles 23 and 139 of the CPC), the court at the place of the crime can have jurisdiction. Judges also apply the objective ubiquity theory to locate the crime.

[54] For a detailed discussion of this problem and potential solutions, see H.W.K. KASPERSEN, "Cybercrime and Internet jurisdiction (Draft discussion paper of 5 March 2009 prepared in the framework of the Project on Cybercrime of the Council of Europe)", 19 et seq., www.coe.int/cybercrime; S.W. BRENNER, "The Next Step: Prioritising Jurisdiction" in *Cybercrime and Jurisdiction. A Global Survey*, The Hague, T.M.C. Asser Press, 2006, 327-349; S.W. BRENNER and B.J. KOOPS, "Approaches to Cybercrime Jurisdiction", *Journal of High Technology Law* 2004, issue 1, 1-46.

[55] H.W.K. KASPERSEN, "Cybercrime and Internet jurisdiction (Draft discussion paper of 5 March 2009 prepared in the framework of the Project on Cybercrime of the Council of Europe)", 9, www.coe.int/cybercrime.

[56] See Article 550 *bis* Belgian CC. In this case, the perpetrator was prosecuted for hacking with the aggravating circumstance of damaging the IT system or data (Article 550 *bis*, §3, 3° Belgian CC). Strictly speaking, this constitutive effect took place on the servers on which the data were stored.

basing its competence on the constitutive effect of the offence of computer forgery, the disadvantage caused.[57] It could have rested on the argument that the victim experienced this disadvantage at the location of his centre of interest, which is generally the place where he normally resides.[58]

16. NEED FOR SEPARATE 'CYBER JURISDICTION'? - The days when a crime was a local event are gone for good. The internet, the worldwide network of computer networks, has linked places, people and machinery around the world together in an unprecedented way. It is an unparalleled means of communication. It challenges the accepted territorial grounds for jurisdiction and this peculiarity complicates the location of offences and offenders. When victims or prosecuting authorities already have a lead, such as an email address or an IP address, this is often irrelevant in pinpointing the location of the perpetrator or the crime, and sometimes it can even be misleading. An IP address or a URL does not necessarily, for example, match a physical location. A ".be" website can be operated perfectly well from a server in Belarus. Software such as TOR[59] reinforces this lack of borders. It makes it extremely difficult to pinpoint the physical location of the person behind the computer screen. This makes some territorial jurisdiction theories, such as the doctrine of territorially located criminal behaviour, difficult to apply. This locates the crime where the perpetrator physically performed the criminal conduct, and this is what makes it so difficult to discover in the context of cyberspace.
On the other hand, we have seen States such as Belgium claim jurisdiction on the basis of the effects of the crime. A criminal act can take place in cyberspace in many countries at the same time, and in the same way, and create damage in all these countries, for example the spread of viruses, hate mail or racist statements on an internet forum. The ease with which these crimes spread around the world is hitherto unknown.

Must we adapt our rules of jurisdiction to suit these future technologies or even create new rules of jurisdiction for cybercrime? We are of the opinion that a separate system of jurisdiction for cybercrime would not be feasible because we should not lose sight of the fact that the overwhelming majority of cybercrime is ultimately just "old" crime in a new guise. Online fraud is and always will be fraud. Transferring money from the black market via e-banking is and always will be money laundering. The legal interests to be protected are the same, whether the context is online or offline: property, integrity, trust, morality, security, etc. Intrusion into someone else's computer breaches the integrity of that system, just as intrusion into someone else's house breaches the integrity of the home. Increasing digitisation will mean that, in the future, the majority of crimes will be committed with the help of/directed towards an information system: this is because we are gradually exchanging the old metal key for the digital access code. Rather than set up a separate system for this, we are opting to "update" the existing principles to make them workable in a cyber-context.[60]
This is also the vision that underlies the Convention on Cybercrime, which deliberately does not provide for a separate system of jurisdiction for cybercrime. Its authors found that the Member States had to retain their choice because then they could opt not to criminalise some cybercrimes specifically, but "*in the form of a technology-independent provision, such as could happen in the case of the implementation of Articles 7, 8, 9 and 10. A Party may wish not to apply all the principles of Article 22 to traditional crimes and their variants*."[61] It would seem better, in our opinion, to look at the constitutive objective effects or objective elements (*actus reus*) of the crime to ascertain whether or not they exhibit a *substantial link* with a given territory (*see infra*, no. 24).[62]

---

[57] Criminal Court of Liège, 17 September 2003, *Revue de jurisprudence de Liège, Mons et Bruxelles* 2003, issue 35, 1542. As is the case with 'classic' forgery of written documents, a potential disadvantage is sufficient in the case of computer fraud. The Belgian criminal courts cannot, however, use the potential disadvantage to locate an offence because of its nature. Court of Cassation, 7 June 2011, P.11.0172.N, *Nullum Crimen* 2012, 68, note S. DEWULF, "Grenzen aan (extra)territoriale rechtsmacht van België".

[58] See Court of Justice, 25 October 2011, C-509/09, *eDate Advertising GmbH/X* and Court of Justice, 25 October 2011, C-161/10, *Olivier Martinez and Robert Martinez/MGN Limited*. These were not criminal cases, but they did relate to an action that caused damage (an unlawful act). When damage is a constitutive effect of an offence, the same reasoning can, in our opinion, be applied.

[59] The Onion Router. This software allows entirely anonymous internet surfing and communication.

[60] See also H.W.K. KASPERSEN, "Cybercrime and Internet jurisdiction (Draft discussion paper prepared in the framework of the Project on Cybercrime of the Council of Europe)", www.coe.int/cybercrime.

[61] H.W.K. KASPERSEN, "Cybercrime and Internet jurisdiction (Draft discussion paper of 5 March 2009 prepared in the framework of the Project on Cybercrime of the Council of Europe)", 15, www.coe.int/cybercrime; H.W.K. KASPERSEN, "Jurisdiction in the cybercrime convention" in *Cybercrime and Jurisdiction. A Global Survey*, The Hague, T.M.C. Asser Press, 2006, 17.

[62] If this means that many offences cannot be located in Belgium, the legislator should consider establishing extraterritorial jurisdiction over cybercrime in the First Title of the Criminal Procedure Code. He could do so, for example, on the basis of the passive personality principle (Belgian victim) or protective principle. The question would then remain as to what should be done with the condition in Article 12 of the First Title of the CPC (encounter with the suspect in

2. *Where is the omission offence in Article 46 bis, §2 of the CPC committed?*

17. 'VIRTUAL' PRESENCE AS A TERRITORIAL LINK? - The first point for discussion in the *Yahoo* case is that of whether the company committed the offence on Belgian territory (Article 3 Belgian CC). When we use the objective ubiquity theory to see if this is the case, which is presumably the idea, we have to ask: "Where did Yahoo omit to cooperate with the Belgian judicial authorities?"
Yahoo itself said that it was not present on Belgian territory and that it could not, therefore, have committed a crime on said Belgian territory (Article 3 Belgian CC). From its absence in Belgium, the company therefore deduces that one cannot speak of a *Belgian offence*. According to the prosecutor, Yahoo was indeed present in Belgium and this is one of the reasons why the crime was committed in Belgium (see *supra*, no. 4).
The prosecutor, followed by the criminal court, sees Yahoo as a foreigner that "is present" in Belgium. In his eyes, Yahoo is like the foreigner who drives on Belgian roads and commits a speeding offence. He deduces the "virtual presence" of Yahoo from the fact that it "provides services" in Belgium: because Yahoo has an "economic-virtual" presence in Belgium, it also has a "judicial-virtual" presence. He then equates this so-called "virtual" presence to an actual "physical" presence. Through the virtual world of "cyberspace", he brings Yahoo to Belgium and, in his eyes, the company commits an offence here.
On this point, our view of the internet differs from the prosecutor's. The internet is and remains a means of communication between real people in the real world, who find themselves in a given (possibly different) jurisdiction.[63] Providing communication services over the internet in Belgium from abroad is not the same as having an actual "presence" here. One could compare the situation to that of internet banking: Belgians can have an account with a foreign internet bank. In that case, the bank is providing services in Belgium, but this does not mean that it is actually present in the country.
This focus of the discussion on Yahoo's presence or absence in Belgium is surprising, now that, in our opinion, it is not particularly relevant to the 'geolocation' of the omission offence, as a (legal) person need not necessarily "be" in Belgium to commit a crime on Belgian territory (see *supra*, no. 12). To determine whether or not Yahoo committed an offence that can be located in Belgium, it must be possible to locate one of the objective elements in Belgium (see *supra*, the objective ubiquity theory): if someone in Belize transfers illegal money from a Swiss bank account to an account in Belgium, he is committing a Belgian money laundering offence (Article 505 Belgian CC). If a Chinese person in Singapore deliberately manipulates the computer system of a Belgian hospital to kill a patient, he commits a murder in Belgium. Everything depends on the location of the objective elements of the crime.

18. LOCATION OF THE DUTY TO COOPERATE. - A 'duty to cooperate' seems to imply a sort of obligation actively to act on the part of the person involved.[64] This obligation on the part of the operator or provider to disclose information does not, however, come into being until after the Public Prosecutor has issued a request. If the operator or provider refuses to cooperate, he commits an offence. Failure to disclose the information within the stipulated period also implies refusal. A failure to meet this obligation is punishable. Article 46 *bis*, §2 Belgian CPC is therefore a 'criminal omission: the operator or provider omits to fulfil a punishable duty to act under the criminal law.

Since by definition there is no active behaviour, no action, it is of course difficult to locate omission offences. Is the place where the person should have acted the place where she became aware of her duty to act or the place where she decided not to act?
According to Belgian law and case-law, the defaulter commits the offence at the place where he is required to fulfil the duty.[65] We see this, for example, in the duty of identification in Article 67 *ter* of the

Belgium). See also U. SIEBER, "*Cybercrime and Jurisdiction* in Germany. The present situation and the need for new solutions" in *Cybercrime and Jurisdiction. A Global Survey*, The Hague, T.M.C. Asser Press, 2006, 207.

[63] See in this regard the interesting discussion in the American literature of the late 1990s on "cyberspace" as a separate space that is not open to regulation. As the *Yahoo* case shows, this discussion is still relevant today and the various standpoints lead to different interpretations of the application (or applicability) of law in internet (criminal) law cases. See, among others, J.L. GOLDSMITH, "Against Cyberanarchy" in *University of Chicago. The law school. Occasional papers*, Chicago, University of Chicago. Law school, 1999, 40, p. 1-37; D.R. JOHNSON and D.G. POST, "Law and Borders - The Rise of Law in Cyberspace", *Stanford Law Review* 1995-96, issue 48, 1367-1402; L. LESSIG, "The Zones of Cyberspace", *Stanford Law Review* 1995-96, issue 48, 1403-1411; T.S. WU, "Cyberspace sovereignty?" *Harvard Journal of Law and* Technology 1997, issue 3, 647-666; D. GOLDSTONE and B.-E. SHAVE, "International dimensions of crimes in cyberspace", *Fordham International Law Journal* 1998, issue 5, 1924-1971.

[64] T. INCALZA, "Strafonderzoek in het digitale tijdperk: zoeking en beslagneming", *Jura Falconis* 2010-11, issue 2, 372.

[65] R. DECLERCQ, "Bevoegdheid" in *Strafrecht en strafvordering. Artikelsgewijze commentaar met overzicht van rechtspraak*, 77. See also in relation to omission to report a birth (Article 361, 2° Belgian CC): Court of Cassation, 31

Road Traffic Act, to which the prosecutor also referred. This provision has much in common with the duty to cooperate in Article 46 *bis* Belgian CPC. The two offences turn a failure to comply with procedural obligations into an offence in its own right (they are a sort of "procedural obstruction offence", a contempt of public authority). Article 67 *ter* of the Road Traffic Act obliges natural persons who represent a legal person in law to disclose the identity of the driver who committed a road traffic offence in Belgium in a vehicle registered to that legal person. The Court of Cassation has confirmed on several occasions that the offence is committed when the offender has not been identified. The place at which the identification is to be received is the place of the offence, not the place where the legal person is based.[66]

The same reasoning applies here. As soon as the operator or provider learns of a *compulsory request* to disclose information there arises an obligation to comply with it. We can assume that he it? has fulfilled this obligation when he discloses the information to the prosecutor. The duty to act therefore applies at the place where the prosecutor is to receive the information.[67] As a consequence, the duty to cooperate can indeed be located in Belgium, even if the person charged with that duty of cooperation is located abroad. Omitting to fulfil this duty is a Belgian territorial offence and it can be committed by Belgians and foreigners alike. But that doesn't solve all of the problems. The next question concerns the party upon whom the duty rests and, in this case, whether Yahoo falls within the scope of this duty (point 3.3.) and, if so, whether Yahoo's duty in this specific case was indeed "activated" (point 4).

3. The ratione personae *scope of the Belgian duty to cooperate*

19. WHO? - This question relates to the personal scope of Article 46 *bis* Belgian CPC: who can receive the Belgian prosecutor order to cooperate on the basis of Article 46 *bis* Belgian CPC and who is then, as a consequence, punishable in case of a failure to comply? There are two sub-questions:

- who is an operator of an electronic communication network or a provider of an electronic communications service in the sense of Article 46 *bis* Belgian CPC (point 3.3.1.)?
- are foreign companies that provide electronic communications services over the internet also subject to the Belgian duty of cooperation (point 3.3.2.)?

A. The concepts "operator of an electronic communication network" and "provider of an electronic communications service"

20. ONLY TRANSMISSION OF COMMUNICATION? - Article 46 *bis* Belgian CPC states that the Public Prosecutor can order the cooperation of "*the operator of an electronic communication network or the provider of an electronic communication service*". The refusal to cooperate (the "obstruction by omission offence") is therefore a 'status-related offence': a person who does not enjoy that status cannot be an offender. In this article, the legislator made deliberate use of the same terminology as Article 2 of the ECA. This is because the intention was to harmonise the various provisions on electronic communication.[68]
When applying the ECA, the court looks at whether the service is (chiefly) designed to transmit signals.[69] Measuring the duty to cooperate in Article 46 *bis* Belgian CPC against this yardstick would seriously limit its scope. An internet user generally requires three things - aside from, that is, a device (phone, computer, etc.) - in order to send email:

- an infrastructure over which email is sent (a network)[70];
- an electronic communication service to transmit the signals[71];

October 2001, P.01.1162 F, *Court of Cassation judgement* 2001, 589; Court of Cassation, 2 October 2002, P.02.635.F, *Court of Cassation judgement* 2002, 497, *Revue de jurisprudence de Liège, Mons et Bruxelles* 2003, 62.

[66] Court of Cassation, 27 April 2010, P.09.1625.N, *Pasicrisie Belge* 2010, issue 4, 1283; *Nullum Crimen* 2011, issue 6, 371, note V. FRANSSEN and S. VAN DYCK; Court of Cassation, 22 April 2008, P.08.0250.N, *Pasicrisie Belge* 2008, issue 4, 986; *Rechtskundig weekblad* 2008-09, issue 33, 1383 note P. ARNOU; *Verkeer, aansprakelijkheid, verzekering* 2008, issue 5, 463; *Nullum Crimen* 2009, issue 2, 123.

[67] P. ARNOU, "De plaats waar de identiteit moet worden meegedeeld van de bestuurder die een overtreding heeft begaan met een motorvoertuig dat toebehoort aan een rechtspersoon", *Rechtskundig weekblad* 2008-09, issue 33, 1384.

[68] On this, see the detailed statement of Solicitor General De Swaef, *Nullum Crimen* 2011, issue 1, 84, 79-84. See also *Parliamentary Documents* Senate 2005-2006, 3-1824/2; P. DE HERT and G. BOULET, "Yahoo! moet meewerken met Belgische prosecutor", *De Juristenkrant* 2012, issue 253, 8.

[69] N. VANDEZANDE, "Yahoo! als operator of verstrekker", *Auteurs en media* 2011, issue 2, 222.

[70] In Belgium, these are Belgacom and Telenet for the internet (see the statement of Solicitor General De Swaef, *Nullum Crimen* 2011, issue 1, 84, no. 10).

[71] E.g. Scarlet, Belgacom, Telenet, Evonet, Toledo Telecom, edpnet, Belnet, etc.

- an application or program to send, receive and store email.[72]

Only the first two are services in the strict sense, designed principally to transmit signals. Yahoo's free webmail system belongs to the third category. This webmail is a software application that enables users to send and receive email via a web browser or Internet Access Provider[73] without having to use a separate email program (e.g. Outlook, Eudora, etc.). They use HTML, so that it works in the same way as a website does. The beauty of this is that you can use it to send and receive email anywhere in the world. The email account in question is (probably)[74] located, in the case of Yahoo, on its servers in the United States. For example, you can use your own computer (with its own IP address) in Turkmenistan to log into the Yahoo website (mail account) in the US, and send email to anywhere in the world from there.

Yahoo only provides its customers with an application. In the process, it makes use of the existing network and does not transmit the signals itself. Were we to limit the scope of Article 46 *bis* Belgian CPC to the party responsible for transmitting the signals (Belgacom, Telenet, etc.), companies like Yahoo, Hotmail and Google would not have a duty to cooperate. For that matter, these companies also record information that could be extremely helpful in detecting (the perpetrators of) a crime, such as the IP address that someone used when he or she "created" the email account. When an offence is committed using fictive email addresses, the webmail (banksecurity@yahoo.com, littlepervert@hotmail.com, teleromeo@telenet.be, etc.) is often the only lead the investigators have to start with. If they know the IP address, they can then link it to an internet access provider. It too has a duty to cooperate (see *supra*, no. 3) and can hopefully identify the subscriber with that IP address. The cooperation of the webmail provider is therefore a necessary prior step to obtain the cooperation of the internet access provider and is crucial to the efficiency of the cyber-investigation.

21. WEBMAIL PROVIDERS TOO. – Opinion on the geographical scope of the duty to cooperate was deeply divided. Yahoo adopted the strict interpretation and was followed in this by the Ghent Court of Appeal and Advocate General DE SWAEF. In his written conclusions, the Advocate General gave an in-depth analysis of the legal framework of investigative practice in relation to electronic communication and developments in the law.[75] He discussed the arguments for and against a narrow interpretation of the notion of "provider of an electronic communication service". In the end, he concluded that the legislator had in mind only those service providers that transmit communication data. The Public Prosecutor argued instead in favour of a broad interpretation and the Court of Cassation agreed. Providers of an electronic communication service in the sense of Article 46 *bis* Belgian CPC are, according to the Court:

- the operators of electronic communications networks in the sense of the ECA;
- anyone who provides a service consisting fully or partially in the transmission of signals via electronic communication networks;
- *anyone who allows its customers to obtain or disseminate information through an electronic network*.

The interpretation of the Court of Cassation is therefore much broader than the scope of Article 2 of the ECA. This means that webmail providers such as Yahoo also fall within the personal scope of the duty to cooperate. The company is not itself able to transmit communication, but it allows its users to obtain and disseminate information. In this sense, it is an electronic communications provider.

22. JUSTIFIED CRITICISM? - This judgement met with criticism from legal commentators. According to VANDEZANDE, it came down to a forbidden analogical interpretation that also went against legislative intent.[76] We are of the opinion, however, that the Court's interpretation is certainly defensible in the light of the conceptual autonomy of criminal law. Admittedly, the line between a forbidden analogical interpretation and the autonomy of criminal law is a fine one. In conformance with the latter, the criminal judge can give other meanings to the concepts from other areas of law, bearing in mind the legal interest which the criminal statute seeks to protect.[77] The legal interest that the legislator seeks to protect with this offence is clear: an efficient (or more efficient) fight against crime. The increasing communication options open to criminals and the provision of services by private companies makes the cooperation necessary of those private companies and, specifically, their compulsory contribution to identification.[78] From the criminal (procedural) law perspective, a wider scope for duties to cooperate with criminal investigations

[72] E.g. Hotmail, Gmail, Yahoo!Mail, etc.
[73] E.g. Internet Explorer, Mozilla Firefox, etc.
[74] "Probably" because applications such as cloud computing divide the data and store them dynamically.
[75] Statement of Solicitor General De Swaef, *Nullum Crimen* 2011, issue 1, 79 et seq.
[76] N. VANDEZANDE, "Yahoo! als operator of verstrekker", *Auteurs en media* 2011, issue 2, 223.
[77] Court of Cassation, 27 March 1995, *Court of Cassation judgement* 1995, no. 170; F. VERBRUGGEN and R. VERSTRAETEN, *Strafrecht en Straf procesrecht voor bachelors*, Antwerp, Maklu, 2012, 7.
[78] See also explanatory memorandum to the bill amending the Act of 30 June 1994 on the protection of personal privacy against eavesdropping, surveillance and recording of private communication and telecommunication, *Parliamentary Documents* Chamber of Representatives 1996-97, no. 49-1075/1, 2.

than that afforded under Article 2 of the ECA is a good thing. Without it, the identification of many cybercriminals and shady webmail users would not be possible: they would enjoy impunity. It can hardly be said that this was legislative intent. It would also create a bizarre inequality in the field. Investigators would be able to identify users of a Telenet email address, but not those of a Yahoo email address, as the former is a Belgian corporation and the latter is not.
Moreover, the Court chose an interpretation which is in conformity with the Cybercrime Convention[79]. Indeed Article 18 of this convention compels States to authorise their competent authorities to order "*that a service provider that offers its services in the territory of the party to submit subscriber information relating to such services in that service provider's possession or control*". Therefore, the convention does not speak of operators, but of "service providers". According to Article 1, a service provider is:

- any public of private entity that provides to users of its service the ability to communicate by means of a computer system;
- any other entity that processes or stores computer data on behalf of such communications service or users of such service.

Given that webmail is a computer system allowing users to communicate, this falls within the scope of the Convention on Cybercrime and Belgium is obliged to facilitate the disclosure of identification data.

The interpretation of the Court and the definition given by the Convention on Cybercrime are rooted in the reality of electronic communication, more particularly email traffic, whereby networks, signal transmission and applications are needed to achieve communication over the internet. The concepts of the ECA are too limited from this perspective. Therefore, we can only subscribe to the interpretation offered by the Court of Cassation.

B. Foreign based service providers too?

23. CONSEQUENCES OF A BROAD SCOPE. - This broad interpretation of the concepts of "operator" and "provider" in relation to the duty to cooperate has one important consequence. It can quickly be extended to foreign service providers, simply because of the possibilities afforded by the internet. This is because in order to provide communications services, service providers need not necessarily be based in Belgium. It raises the question as to whether foreign companies can also be compelled to cooperate with the Belgian police authorities under the threat of a sanction.

24. PROVISION OF SERVICES. - Under a broad interpretation of the territoriality principle, we might say that companies that use the internet to do business around the world should abide by the laws of every country because their actions (can) have an effect everywhere. This means that their ubiquity leads to territorial jurisdiction on the part of every State in the world.
But it would be going a step too far to suppose that mere "virtual" presence is enough to create territorial presence. A claim of jurisdiction must also be reasonable.[80] We think it would be too much to expect companies with a presence on the internet to abide by all the rules set by all the world's countries purely because they have a website that can be accessed from anywhere in the world. This is because a website's global accessibility is not always something over which they have any control, whereas internet users do. Moreover, it makes these companies dependent on an incoherent and potentially conflicting legal framework (see *supra*, no. 13). This legal uncertainty might even discourage the free flow of information (and provision of services).[81] Nor does it always simply follow that it would suffice for companies that provide internet services around the globe to abide by the rules of the country of their registered office and/or in which they keep their servers. This might threaten a "race to the bottom" where internet players set themselves up in an "internet safe haven" and do business with the rest of the planet

[79] The Budapest Convention of 23 November 2001 on the combatting of crime in relation to electronic networks. This convention served as the inspiration for amendments of Belgian law. Eleven years later, Belgium has finally ratified the convention (Act of 3 August 2012 endorsing the convention on computer crime, agreed in Budapest on 23 November 2001, *Belgian Official Journal* 21 November 2012). This convention came into effect on 1 December 2012.
[80] C. RYNGAERT, *Jurisdiction in International Law*, Oxford, Oxford University Press, 2008, 134 et seq.
[81] See the statement of Solicitor General P. Cruz Villalón, 29 March 2011, in the cases *eDate Advertising GmbH and Martinez*, www.curia.europa.eu (Court of Justice, 25 October 2011, C-509/ 09, *eDate Advertising GmbH/X*, and Court of Justice, 25 October 2011, C-161/10, *Olivier Martinez and Robert Martinez/MGN Limited*).

from there.[82] Nor should the victims of cybercrime be left out in the cold.[83] The government must strike a balance between legal certainty for service providers and legal protection for victims.

Jurisdiction requires a substantial link between a given country and a service provider. This link must also be technologically neutral.[84] If it is not, new technological advancements will threaten to supersede the claims of jurisdiction.[85] Article 18 of the Convention on Cybercrime applies the duty to cooperate to a service provider "*offering its services in the territory of the Party*". Similar links are to be found in Section 403 of the American Restatement (Third) of Foreign Relations Law of the United States, an important guideline in problems relating to jurisdiction. The Restatement says that legal jurisdiction is reasonable on the basis of "*(b) the connections, such as nationality, residence, or economic activity[86], between the regulating State and the person principally responsible for the activity to be regulated*".

From this, we can deduce that if a company offers services on Belgian territory consisting in the receiving or disseminating of information via an electronic network, it is reasonable for the Belgian legislator to subject it to a duty to cooperate. A duty such as this would appear justified when it comes to effectively fighting crime.[87] It is therefore desirable to determine when service providers offer their services on Belgian territory. This problem is not in itself new. The Court of Justice of the European Union has already had to determine in several e-commence cases whether or not a contractor, when offering his services via the internet, was also "directing his activities" at a particular Member State. These judgements might also be a source of inspiration.[88]

25. "TO ACTIVELY DIRECT TO" - In the case of *Pammer*[89], an Austrian consumer had booked a trip via the website of a German company. A dispute arose and the Austrian summoned the German company

[82] See also in this sense ECHR, 18 October 2005, *Perrin/United Kingdom*, no. 5446/06, www.echr.coe.int. To date, this is the only known judgement by the Court in relation to internet jurisdiction. The case involved a French man, residing in the United Kingdom, who administrated the pornographic website of an American company from the United Kingdom. He was prosecuted in the United Kingdom for publishing pornographic images on the internet. He argued that the United Kingdom did not have jurisdiction because it was an American company and the information was published on the internet in the US. The Court dismissed Perrin's argument of legal uncertainty and ruled that Perrin, as a resident of the United Kingdom, could not argue that the laws of the United Kingdom were not reasonably open to him. The Court decided that if the courts of the United Kingdom could only judge "publication-related cases", when the place of *publication* was situated in the United Kingdom, then this would lead to "safe havens".

[83] See *supra*, footnote 5.

[84] See on this principle B.J. KOOPS, "Should ICT Regulation be Technology-Neutral?" in B.J. KOOPS, M. LIPS, C. PRINS and M. SCHELLEKENS, *Starting Points for ICT Regulation: deconstructing policy one-liners*, T.M.C. Asser Press, The Hague, 2006, 77-108.

[85] Were we to opt, for example, for the place where the server is located as a necessary territorial link, then applications such as cloud computing and mobile internet would threaten to make the theory completely unworkable. See also *supra*, no. 16 relating to the vision of the Cybercrime Conventions and H.W.K. KASPERSEN, "Jurisdiction in the cybercrime convention" in *Cybercrime and Jurisdiction. A Global Survey*, The Hague, T.M.C. Asser Press, 2006, 17.

[86] This is our own underlining.

[87] See for example, the jurisprudence of the European Court of Justice on internet gambling, in which the Court accepts under certain conditions monopolies and other restrictions regarding the number of providers in the gambling game sector. Restrictions on freedom of services are, according to the Court, justified by the objective of fighting fraud and crime. These national regulations can also apply to foreign companies that offer these activities in a given Member State over the internet. See also, among others, Court of Justice, 15 September 2011, C-347/09, *15 September 2011, Dickinger and Ömer*; Court of Justice, 30 June 2011, C-212/08, *Zeturf Ltd./Prime Minister*; Court of Justice, 8 September 2010, C-46/08, *Carmen Media Group Ltd./Land Schleswig-Holstein en Innenminister des Landes Schleswig-Holstein*; Court of Justice, 3 June 2010, C-258/08, *Ladbrokes Betting & Gaming Ltd. and Ladbrokes International Ltd./Stichting de Nationale Sporttotalisator*; Court of Justice, 3 June 2010, C-203/08, *Sporting Exchange Ltd./Minister for Justice and the Stichting de Nationale Sporttotalisator*; Court of Justice, 8 September 2009, C-42/07, *Liga Portuguesa de Futebol Profissional, Bwin International Ltd./Departamento de Jogos da Santa Casada Misericórdia de Lisbo*; Court of Justice, 6 March 2007, C-338/04, C-359/04 and C-360/04, *Placanica et al*. In the *Stoβ;* judgement, the Court judged that the State in question would have to make the option of offering these services on its territory via the internet dependent on a licence issued by its own authorities. Court of Justice, 8 September 2010, C-316/07, C-358/07-C-360/07, C-409/07 and C-410/07, *Stoβ; et al./Wetteraukreis en Kulpa Automatenservice Asperg GmbH et al./Land Baden-Württemberg*.

[88] We will have to wait and see what view the European Court of Human Rights takes on internet jurisdiction. In a recent overview of the Court's internet case law, the Research Division noted that there are few cases relating to internet jurisdiction to date. The only example is the *Perrin* judgement that we have already cited (see *supra*, footnote 73). The Research Division does, however, refer to the *Ben El Mahi* judgement over the Danish Mohammed cartoons, in which the Court judged that there was no jurisdictional link between the complainants and Denmark. In the report, the Research Division remarked that this decision could be relevant to future internet cases. ECHR, 11 December 2006, *Ben El Mahi et al./Denmark*, no. 5853/06. See Research Division "Internet: case-law of the European Court of Human Rights", 5, www.echr.coe.int (Case-law/Case-Law Analysis/Research reports).

[89] Court of Justice, 7 December 2010, C-585/08, *Peter Pammer/Reederei Karl Schlüter GmbH & Co. KG*.

before the Austrian court. The German company contended that it pursued no commercial or professional activity in Austria. In the case of *Alpenhof*[90], a German had booked a room in an Austrian hotel via the hotel's website. The German was not satisfied and refused to pay. The Austrian hotel then claimed payment before the Austrian court. In both cases, the defendant contested the jurisdiction of the Austrian court.[91]
The Austrian court therefore asked the Court of Justice whether a company also "directs its activities" to a consumer in another Member State when it offers its services over the internet. The European Court answered that the mere fact that a company offers its services over the internet does not imply that these services are also directed at other Member States. Mere "virtual" presence via an internet site is in itself insufficient to establish a territorial link. What counts for the Court is whether the company expressed its wish to enter into commercial relations with consumers in other Member States.[92] The Court gives the following as indications of this wish[93]:

- paying a search engine advertising service to ensure easier access to the site;
- the internationally directed nature of the activity. This might be seen from the sort of activity (e.g. tourism), but also the way in which a company profiles its activities as transborder, for example, the use of a telephone number with an international dialling code, a top level domain name such as ".com" or ".eu", the option to use a language or currency other than those normally used in the company's Member State;
- the nature of the advertising on the page. This is an important indicator of geographical targeting because the company often derives its income from this.[94]

These are all cases in which a service provider might reasonably ensure that its website contains information that is *objectively relevant* in a given geographical area. In other words, the online information has a distinct meaning or value in a given area.[95]

A similar theory of jurisdiction can be found in the American "sliding scale" *Zippo*'s test.[96] This theory sees the internet as a worldwide forum that brings people and companies in contact with each other and looks at the relationship that is established each time. According to this analysis, courts must decide personal jurisdiction from the level and nature of the commercial activities on the internet, ranging from "passively" to "actively" doing business.[97] In broad terms, this gives us three sorts of website. To start with, a website can actively direct itself to the citizens of a given country. This unambiguous wish to enter into commercial relations with people from that country can suffice as a territorial condition. But a website can also have a passive presence. This does, of course, mean that the website can be accessed from anywhere, but this does not create a territorial link with countries from which the site is viewed. This avoids universal jurisdiction claims from all countries over such websites. Finally, a website can also be interactive. This means that the user exchanges information with the administrator. To determine jurisdiction, the level of interaction and the commercial nature of the information are important. According to this "sliding scale" test, a company will have to respect the laws of any country that it targets commercially.

---

[90] Court of Justice, 7 December 2010, C-144/09, *Hotel Alpenhof GesmbH/Oliver Heller*.
[91] The EU regulation on legal jurisdiction in civil and commercial matters states that the consumer may lodge a claim in the Member State of his residence if the contractor "directs its activities towards" that Member State.
[92] The Court recently applied this theory in a case on trademark law. It ruled that the national judge must check on a case-by-case basis whether there are any relevant indications that the sale offer or advertisement displayed on an electronic marketplace, which can be accessed from the territory contested by the brand, is *intended* for consumers located there. Court of Justice, 12 July 2011, C-324/09, *L'Oréal SA et al./eBay International AG et al*.
[93] See also the statement of Solicitor General N. Jääskinen, 10 March 2011, Court of Justice C-462/09, *Stichting de Thuiskopie/Mijndert van der Lee, Hananja van der Lee and Opus Supplies Deutschland GmbH*.
[94] Internet service providers adapt their websites, with the help of geo-location software for example, to suit their users' locations. Y. POULLET, "Towards confidence: views from Brussels: a European Internet Law? Some thoughts on the specific nature of the European regulatory approach to cyberspace" in G. CHATILLON, *Internet International Law. International and European Studies and Comments*, Brussels, Bruylant, 2005, 148-149.
[95] Statement of Solicitor General P. Cruz Villalón, 29 March 2011, in the cases *eDate Advertising GmbH and Martinez*, www.curia.europa.eu (Court of Justice, 25 October 2011, C-509/09, *eDate Advertising GmbH/X* and Court of Justice, 25 October 2011, C-161/10, *Olivier Martinez and Robert Martinez/MGN Limited*).
[96] The "minimum contact test" is applied here in internet cases. Under the minimum contact test, it is important to ascertain the extent to which the perpetrator carried out acts in a given State and the relationship between these actions and the claim for damages. See A.M. SACHVEDA, "International jurisdiction in cyberspace: a comparative perspective", *Computer and Telecommunications Law Review* 2007, 248 et seq.; M. SADAAT, "Jurisdiction and the Internet after Gutnick and Yahoo!", *Journal of Information, Law and Technology* 2005, 1717 (http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2005_1/saadat/).
[97] J.H. GRAHAM SMITH, *Internet law and regulation*, London, Sweet & Maxwell, 2002, 347.

26. AND YAHOO? - If we apply these principles to the *Yahoo* case, we note that the Public Prosecutor's position rests on the jurisprudence of the Court of Justice. In his eyes, Yahoo is subject to the Belgian duty to cooperate because the company is economically active in Belgium. The prosecutor stresses that Yahoo uses the internet to direct itself commercially to Belgian citizens. For example, the company registers a user's IP address and is able to locate it. Yahoo then adapts its services to suit the user's location. When users log in to their webmail from Belgium, Yahoo adapts its site to the assumed needs of these Belgian internet users. It provides free-of-charge services for its users because its entire profits derive from such form of advertising.

Therefore Yahoo directs itself actively to the Belgian consumer and so offers services in Belgium, even though it is not present here. We might also conclude that the place of establishment does not determine the territorial and personal scope of the duty to cooperate. Yahoo is not present in Belgium, but can be required to cooperate with the Belgian police authorities. The broad interpretation of the territoriality principle, combined with the criteria of the Court of Justice, leads us to conclude that Article 46 *bis* of the Belgian CPC also applies to foreign providers of electronic communications services when they actively offer their services in Belgium.

This does not necessarily mean that these foreign companies will always be sanctioned when they fail to satisfy a legitimate Belgian request for cooperation. The request might, for example, be inconsistent with the legislation of the country in which the company is based and so give rise to a conflict of laws.[98] The company could in such a case argue that its legal obligations under the law of the country in which it is based warrant a refusal to cooperate with the Belgian State (Article 70 Belgian CC). Countries like Belgium used to pay no attention to foreign law when crimes were committed on their own territory, but in an increasingly globalised world with more and more positive jurisdiction conflicts between States, this approach is no longer sustainable. The new trend is identifiable, for example, from the increasing importance of transborder *ne bis in idem* rules, which also apply to Belgian territorial crimes.[99]

IV. Procedural criminal jurisdiction: I bark, but only my partner can bite

27. ENFORCEMENT OF THE DUTY TO COOPERATE. - In the above we have tried to show that Yahoo can fall within the territorial and personal scope of the Belgian offence in Article 46 *bis*, §2 Belgian CPC and can be prosecuted in Belgium for that offence. However, one can talk of a punishable refusal to cooperate only if a procedural duty to cooperate has effectively arisen. On this point, we find that substantive criminal jurisdiction is interwoven with procedural profiles. We are left, therefore, with the question of how Belgium can impose this duty to cooperate on a foreign subject based in a foreign country. This is because the enforcement powers of the Belgian authorities do not stretch beyond the national borders. Where do these investigative powers end in this "borderless" digital space? When does this duty to cooperate arise for Yahoo? How is it triggered? Can a company based in a foreign country ever be required to respond to a *Belgian* request for cooperation? If so, when? How can the Belgian prosecutor *enforce* the duty to cooperate on foreign companies?
Below, we start by setting out the general principles of transborder enforcement (title 1). Then we investigate whether a prosecutor's request under Article 46 *bis* Belgian CPC to a service provider based in a foreign country can be considered as transborder enforcement (title 2). Finally, we test our findings against the omission offence in Article 46 *bis*, §2 Belgian CPC (title 3).

1. Ban on transborder law enforcement?

28. LIMITED PROCEDURAL JURISDICTION. - Up to this point, we have covered only substantive jurisdiction or jurisdiction to prescribe and to adjudicate. Belgium is entitled to oblige foreign service providers that are economically active in its territory to cooperate with the Belgian judicial authorities. But how it can ensure that it actually receives cooperation is another matter. This calls into question the limits of the State's

[98] This concern and the entire judicial issue surrounding it is currently also occupying the Cybercrime Convention Committee (T-CY) of the Council of Europe. See their report "Transborder access and jurisdiction: what are the options?", Report of the Transborder Group adopted by the T-CY on 6 December 2012, 11 et seq. and 44, www.coe.int/TCY.
[99] For example, Article 54 of the Schengen Implementation agreement prevents the prosecution in Belgium of a Belgian territorial offence after a final judgement on that offence in another Schengen country. See also H.W.K. KASPERSEN, "Cybercrime and Internet jurisdiction (Draft discussion paper of 5 March 2009 prepared in the framework of the Project on Cybercrime of the Council of Europe)", 11, www.coe.int/cybercrime.

jurisdiction to enforce, which is a much more sensitive issue.[100] Where the classic *Lotus* judgement was flexible on substantive jurisdiction, a sovereign *claim* to power, it was not flexible on executive jurisdiction, a sovereign *exercise* of power. This jurisdiction "*cannot be exercised by a State outside its territory except by virtue of a permissive rule derived from international custom or from a convention*".[101] States can therefore, in theory, only exercise their procedural powers within the national borders. But, where do these borders end in the digital environment? Once again, territoriality is the criterion that creates problems in an "aterritorial" virtual space. Authorities (just like cybercriminals) can investigate information abroad by digital means without physically having to leave their territory.[102] And, as in the *Yahoo* case, they can request information from a foreign service provider via modern means of communication, under the threat of criminal prosecution if refused. This raises the question of whether, through this, the Belgian prosecutor is exercising jurisdiction outside Belgium. Is he, with a request of this kind, exceeding his Belgian-wide jurisdiction or would this procedure be permissible in the light of international law?

29. NO UNILATERAL ORDERS ON ANOTHER STATE'S TERRITORY. - The territorial scope of the criminal procedure law arises, as does substantive criminal law, from the sovereign equality of the States (see *supra*, no. 13). If a State wishes to conduct an investigation on another's territory, it does in theory require permission.[103] This is why States conclude bilateral or multilateral conventions on mutual legal assistance allowing, for example, to obtain evidence located on another State's territory. Any unilateral exercise of authority in another country's territory outside the framework of these conventions is, theoretically, contrary to international law.[104] The law on legal assistance does not prevent States from exchanging information voluntarily. A merely informal request is not, therefore, contrary to international law. Neither is fulfilment of that foreign request by a private person, for example.[105] But once the request is no longer informal, but an order, that State is exercising direct authority in another State and this violates the principles of international law.

30. NON-PHYSICAL BREACHES OF SOVEREIGNTY. - To what extent do criminal investigative measures constitute a breach of another State's sovereignty? In our opinion, these acts include not only coercive measures implemented *physically* in a foreign country, such as interrogation after deprivation of liberty, a house search or a seizure of property, but any action by the detectives or investigators which results in subjecting someone or something in a foreign country to state powers. With modern means of communication, investigators no longer have to physically travel. They can investigate foreign computer systems from behind their own computer screens in Belgium, for example. An investigation physically carried out in Belgium can, however, have extraterritorial consequences.
The Council of State, when commenting the draft bill regarding computer crime and the introduction of the Belgian investigative method of network search (Article 88 *ter* Belgian CPC), addressed the difficulty of confining procedural jurisdiction in a digital context: "*It is no easy matter to determine the precise effect of this rule on the action of the law or police in relation to computer data, particularly where orders to detect and seize such data are concerned. This problem is not just the result of the ongoing uncertainty that sometimes exists about where computer data are actually located; it also relates to the fact that an*

[100] C. RYNGAERT, *Jurisdiction in International Law*, Oxford, Oxford University Press, 2008, 24-25; P. DE HERT, "Cybercrime and Jurisdiction in Belgium and the Netherlands. Lotus in Cyberspace - Whose Sovereignty is at Stake?" in *Cybercrime and Jurisdiction. A Global Survey*, The Hague, T.M.C. Asser Press, 2006, 102.
[101] Permanent Court of International Justice, 7 September 1927, *SS Lotus* (France/Turkey), *PCIJ Collection of Judgements* 1927, Series A, no. 10, 19. C. RYNGAERT, *Jurisdiction in International Law*, Oxford, Oxford University Press, 2008, 9 and 22 et seq.; C. VAN DEN WYNGAERT, *Strafrecht, Strafprocesrecht en Internationaal Strafrecht in hoofdlijnen*, Antwerp, Maklu, 2006, 1215. This is our own underlining.
[102] See P.L. BELLIA, "Chasing Bits across Borders", *The University of Chicago Legal Forum* 2001, 35-101; C. CONINGS and J.J. OERLEMANS, "Van een netwerk zoeking naar online doorzoeking: grenzeloos of grensverleggend?", *Computerrecht* 2013, 23 et seq.
[103] J. WOUTERS, *Internationaal recht in kort bestek*, Antwerp, Intersentia, 2006, 115; T. VANDER BEKEN, *Forumkeuze in het internationaal strafrecht. Verdeling van misdrijven met aanknopingspunten in verschillende staten*, Antwerp-Apeldoorn, Maklu, 1999, 231; F. THOMAS, *Internationale rechtshulp in strafzaken* in *Algemene praktische rechtsverzameling*, Antwerp, Kluwer Rechtswetenschappen, 1998, 1 and 55.
[104] Unless on the grounds of a permissive rule derived from international practice. Permanent Court of International Justice, 7 September 1927, *SS Lotus* (France/Turkey), *PCIJ Collection of Judgements* 1927, Series A, no. 10, 19. Note that this ban does not generally apply and is not absolutely observed. See T. VANDER BEKEN, *Forumkeuze in het internationaal strafrecht. Verdeling van misdrijven met aanknopingspunten in verschillende staten*, Antwerp-Apeldoorn, Maklu, 1999, 231-251.
[105] Even if that would be inconsistent with local law, e.g. a European company discloses information to a US authority in breach of national or EU legislation. But this is not a matter of international law.

authority, thanks to that very information technology, has the ability to investigate data abroad without physically leaving the territory of the State in which it is located."[106]
Most Member States of the European Union agreed at that time that transborder access to data or networks, if conducted without the permission of the Member State in question, breach the sovereignty of that country and the principles of international law. This is true in particular of data stored on the territory of another State. In this case, all that remains is the traditional path of mutual legal assistance.[107] Intrusions of this kind are best regulated by international agreements.[108]

Article 20 of the EU Convention on mutual legal assistance in criminal matters[109] and Article 32 of the Convention on Cybercrime are examples of international agreements of this kind of non-physical intrusions. They illustrate the broader investigation potential thanks to the use of new communication technologies.[110]
Problems of jurisdiction in criminal investigations had come up when transborder telephone calls were tapped. When a Belgian receives calls from abroad, these calls can be subject to a Belgian tapping procedure without the Belgian investigators having to leave the territory and without them having to rely on foreign jurisdiction. These telephone calls are, however, multiterritorial because the audio signals move through both foreign and Belgian telecommunication networks and a Belgian tapping order can apply to foreign subjects. As DE SMET rightly says, these cases often involve nothing more than "*a trace that 'moves' to another State without Belgian investigators entering the territory of that State. The breach of the other State's sovereignty is less serious than when the police deliberately cross the border to gather evidence on their own initiative*."[111] However, it is more difficult to come to this conclusion when this is done deliberately. According to DE SMET, this violates the principle of good faith and loyalty in international law.[112]
The EU Agreement contains a specific regulation on this. Under Article 20, the authorities of one Member State can tap a telecommunication address that is used on the territory of another Member State provided that they 1) do not require any technical assistance from that Member State in order to do so and 2) inform the Member State in question either before the tap order, if it is known that the targeted person is on the Member State's territory or, in other cases, immediately after they are aware that the person is located on the territory of the notified Member State. Belgium has transposed this into Article 90 *ter*, §§6-7 Belgian CPC.[113] Therefore, even if it is technically possible to record a telephone call from Belgium with no intervention from the other Member State, Belgium recognises the sovereignty of that Member State.[114]

Article 32 of the Convention on Cybercrime regulates the situation in which investigators are able to gain remote access to a foreign network and the data stored therein (see Article 88 *ter* Belgian CPC). The question of whether this was possible unilaterally led to serious discussion during the preliminary negotiations. It was thought by some that the physical location of the computer systems and the data stored there would determine which State had (exclusive) sovereignty. Others were of the opinion that

---

[106] *Parliamentary Documents* Chamber of Representatives, 50-0213/001 and 50-0214/001, 45-47, which also refers to recommendation no. R(95)13 concerning problems of criminal procedure connected with electronic networks.
[107] See P.L. BELLIA, "Chasing Bits across Borders", *The University of Chicago Legal Forum* 2001. See, however, J.L. GOLDSMITH, "The Internet and the Legitimacy of Remote Cross-Border Searches", *The University of Chicago Legal Forum*, Forthcoming. Available via SSRN: http://ssrn.com/abstract=285732 or http://dx.doi.org/10.2139/ssrn.285732 (posted on 13 October 2001).
[108] See also Recommendation R(95)13 concerning problems of criminal procedural law connected with information technology of the Committee of Ministers (of the Council of Europe).
[109] Council Act of 29 May 2000 establishing, in accordance with Article 34 of the Treaty on European Union, the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union, *Official Journal of the European Union - Information and Notices* 197, 12 July 2000. Approved by Article 2 of the Act of 11 May 2005, *Belgian Official Journal* 22 June 2005, *addendum*, *Belgian Official Journal* 23 September 2005 (first edition).
[110] P. DE HERT, "Cybercrime and Jurisdiction in Belgium and the Netherlands. Lotus in Cyberspace - Whose Sovereignty is at Stake?" in *Cybercrime and Jurisdiction. A Global Survey*, The Hague, T.M.C. Asser Press, 2006, 81.
[111] B. DE SMET, "Registratie en lokalisatie van telecommunicatie" in *Strafrecht en strafvordering. Artikelsgewijze commentaar met overzicht van rechtspraak*, 28.
[112] B. DE SMET, "Registratie en lokalisatie van telecommunicatie" in *Strafrecht en strafvordering. Artikelsgewijze commentaar met overzicht van rechtspraak*, 29; I. ONSEA, *De bestrijding van georganiseerde misdaad: de grens tussen waarheidsvinding en grondrechten*, Antwerp, Intersentia, 2003, 421.
[113] P. DE HERT, "Cybercrime and Jurisdiction in Belgium and the Netherlands. Lotus in Cyberspace - Whose Sovereignty is at Stake?" in *Cybercrime and Jurisdiction. A Global Survey*, The Hague, T.M.C. Asser Press, 2006, 82.
[114] P. DE HERT, "Cybercrime and Jurisdiction in Belgium and the Netherlands. Lotus in Cyberspace - Whose Sovereignty is at Stake?" in *Cybercrime and Jurisdiction. A Global Survey*, The Hague, T.M.C. Asser Press, 2006, 83.

these systems were part of global cyberspace and were therefore freely accessible, not only by citizens, but also by the police and judicial authorities.[115]
Eventually, the Member States reached an agreement on just two issues. These kinds of transborder investigations are possible only when 1) the computer data are open to the public or 2) the investigators have obtained the lawful and voluntary consent of the person who has the authority to disclose the information held in that computer system (see Article 32 of the Convention on Cybercrime). The Council of Europe is currently looking at whether Article 32 of the Convention on Cybercrime has been superseded and must be altered out of practical necessity.[116] But, for the time being, no other transborder access to computer data is permitted under international law. Article 39 of the same convention does not, however, preclude Member States from recognising each other broader powers in other conventions. It also states specifically that it has no effect on a party's other rights, restrictions, obligations or responsibilities (Article 39, §3). The parties to the convention explicitly adopted this "saving clause" because they did not want to exclude broader options for transborder investigative work in the future or between willing States.[117] Whatever the case, these other transborder network searches first require consensus between the States involved.

Instead of accessing this information themselves (hypothesis in Article 32 of the Convention on Cybercrime), law enforcement agencies can request these data from service providers. Belgium obliges these companies to cooperate with Belgian law enforcement. This gives rise to the question of whether a request for cooperation from a Belgian law enforcement authority to a service provider based in a foreign country might also be a non-physical, transborder exercise of authority.

2. The transborder order to cooperate as a transborder collection of evidence

31. COMPULSORY MEASURE? - The duty to cooperate arises only after an explicit request is made by the prosecutor or judge (Article 46 *bis*, §1 Belgian CPC, see *supra*, no. 18). This investigative measure was introduced as an alternative to other, more intrusive investigations, such as the search and seizure.[118] Now that much of the "necessary information" for criminal investigations is no longer with the authorities themselves, obligations of this kind to disclose information to the authorities are quite common. They arise in various contexts. The measure is less intrusive than a search, for example, but it is still a form of coercion.[119] To make the request in Article 46 *bis*, §1 of the Belgian CPC enforceable, the Belgian legislator has introduced an offence for the refusal to cooperate (§2). The threat of a penalty gives the request an undeniably compulsory character. Once again, we can take Article 67 *ter* of the Road Traffic Act as an example (see *supra*, no. 18). In the various cases in which the European Court of Human Rights has had to test these duties to disclose information against the non-incrimination principle, it has stressed that measures of this type have a compulsory nature. For example, in the *Weh* case, the Court ruled that "*without a sufficiently concrete link with these criminal proceedings the use of compulsory powers (i.e.* the imposition of a fine*) to obtain information does not raise an issue with regard to the applicant's right to remain silent and the privilege against self-incrimination*".[120] In *O'Halloran* and *Francis*, the Court reiterated: "*The court accepts that the compulsion was of a direct nature, as was the compulsion in other cases in which fines were threatened or imposed for failure to provide information*."[121]
The request for information is not, therefore, an informal request, but the competent authority does exercise coercive powers on the person addressed. This is why it is better to speak of an "order to cooperate" in relation to Article 46 *bis*, §1 Belgian CPC.[122] The compulsory power of the investigative measure ensues from the very threat of imposition of a fine for a failure to fulfil the duty to disclose information.

32. LOCATION OF COERCION.- The next question in the *Yahoo* case is where the Public Prosecutor exercised this compulsory power: *in Belgium* or *abroad*? In directing the request to the American company based in the US, was the prosecutor actually conducting an investigative act on American territory? The

[115] H.W.K. KASPERSEN, "Jurisdiction in the Cybercrime Convention" in *Cybercrime and Jurisdiction. A Global Survey*, The Hague, T.M.C. Asser Press, 2006, 20.
[116] CYBERCRIME CONVENTION COMMITTEE (T-CY), "Transborder access and jurisdiction: what are the options?", Report of the Transborder Group adopted by the T-CY on 6 December 2012, www.coe.int/TCY.
[117] Explanatory Report to the Cybercrime Convention, §293.
[118] See Explanatory Report to the Cybercrime Convention, §170.
[119] This also comes up in §11 of the Explanatory Report to the Convention on Cybercrime: "(…) iv. the use, including the possibility of transborder use, and the applicability of coercive powers in a technological environment, e.g. (…) requiring service providers to comply with special obligations (…)".
[120] ECHR, 8 April 2004, *Weh/Austria*, consideration 56.
[121] ECHR, 29 June 2007, *O'Halloran and Francis/United Kingdom*, consideration 57.
[122] T. INCALZA, "Strafonderzoek in het digitale tijdperk: zoeking en beslagneming", *Jura Falconis* 2010-11, issue 2, 372.

prosecutor does not believe so because in his eyes, the American company need simply fulfil the Belgian legal duty to cooperate in Belgium (see *supra*, no. 17). Once a company falls within the territorial and personal operating sphere of the omission punishable under Article 46 *bis* Belgian CPC, it is required to bring the information to Belgium when so requested by the prosecutor. The offence is committed at the place where the prosecutor should have received the information, i.e. in Belgium. The prosecutor addressed his request *in Belgium* to a US subject encountered *in Belgium* and Yahoo is required to fulfil this request *in Belgium*.
The prosecutor compares this to Article 67 *ter* of the Road Traffic Act. As we have said above, the Court of Cassation had already ruled on several occasions that the place of the offence of non-cooperation is the place where the Belgian authority is to receive the information.[123] According to the prosecutor, there is also, in relation to the information to be disclosed, a duty to bring them to Belgium, regardless of the place at which the person subject to the duty is based. The prosecutor does not therefore deny that the requested information is in the United States, but in his view the Belgian law requires Yahoo to bring it to Belgium.

In our opinion, the latter is indeed correct, *provided that* the Belgian prosecutor's request did indeed create a duty to cooperate on the part of Yahoo. But the prosecutor has put the cart (punishment for non-cooperative behaviour) before the horse (a duty to cooperate that is binding on the person in question). We agree with his position that, on the basis of Article 23, paragraph 1 of the Belgian CPC, he has the power to prosecute Yahoo if the latter has committed a Belgian offence of failing to fulfil the duty of cooperation. The prosecutor requested Yahoo's cooperation in the framework of an investigation of internet fraud in Dendermonde, in which the perpetrators had made use of communication services provided by Yahoo in Belgium. Yahoo therefore came *ratione personae* under the omission offence of Article 46 *bis* Belgian CPC (jurisdiction to prescribe) and the place of the offence is the place at which the information is to be received (jurisdiction to adjudicate). The duty to cooperate must indeed be fulfilled *in Belgium*. From this, the prosecutor deduces that he did not have to request the information via a letter rogatory to the American authorities, but that Yahoo was required to "bring" them to Belgium after an ordinary request. As we see it, this is where the problem lies: he believes that substantive jurisdiction, i.e. that the international law that allows Belgian judicial authorities to "bark" beyond their borders, also entails full criminal procedure jurisdiction, without any complications. In our opinion, Yahoo is indeed outside Belgium (see *supra*, no. 26) and beyond its borders, Belgium can "bite" (i.e. exercise procedural powers and activate a duty of cooperation) only with the permission or assistance of a local authority. The omission offence located here in Belgium requires a prior, compulsory obligation to "bring" the information. We are of the opinion that a Belgian prosecutor can only obtain this coercion of a *US subject present in the US* with the cooperation or permission of the American government (jurisdiction to enforce). The prosecutor rejects this step as unnecessary. In his eyes, a duty to disclose information exists as soon as he directs himself to the foreign company and it is not fulfilled until he receives the requested information from that company.

If this information resides with a service provider based abroad - in this case Yahoo in the United States - the prosecutor must, as we see it, abide by international law.[124] The competent prosecutor could, of course, send a request under Article 46 *bis* Belgian CPC, regardless of the place at which the service provider is based (see *supra*, no. 26). This location does, however, determine the way in which the prosecutor can enforce cooperation. The prosecutor has no procedural criminal jurisdiction over this foreign company and so cannot issue a direct order or, in this case, enforce the denial of cooperation.
The procedural rules of play do not suddenly change because a failure to fulfil the duty to cooperate is punishable with a fine in Belgium, on the basis of broad rules of substantive jurisdiction.[125] That would

[123] Court of Cassation, 27 April 2010, P.09.1625.N; Court of Cassation, 22 April 2008, P.08.0250.N (see *supra*, footnote 11). The matter of international legal assistance was not raised in either case, however, because they were Belgian companies.
[124] The argument of an "obligation to bring information to the forum" does apply, as we see it, when a Belgian service provider administers the data remotely, with a third party or abroad, for example. In the latter case, in our opinion, that service provider could not argue on the basis of legal assistance that these data are not accessible through it because they are located abroad. Therefore, the location of the data is not decisive under the duty of cooperation. We are of the opinion that this follows from Article 18 of the Cybercrime Convention, which concerns existing data in the possession and under the control of the service provider (see the Explanatory Report to the Cybercrime Convention, §173). Some see this as a breach of the sovereignty of the State in which the data are stored. See CYBERCRIME CONVENTION COMMITTEE (T-CY), "Transborder access and jurisdiction: what are the options?", Report of the Transborder Group adopted by the T-CY on 6 December 2012, 10, www.coe.int/TCY.
[125] See also C. RYNGAERT, *Jurisdiction in International Law*, Oxford, Oxford University Press, 2008, 23: "Likewise, a State cannot resort to legal implementation measures such as penalties, fines, seizures, investigations, or demands for information to give extraterritorial effect to its rules."

circumvent the rules of international legal assistance. Obtaining this foreign evidence [126] is still a matter of international cooperation.[127]
We can compare this to other investigative measures relating to electronic communication, such as telephone traffic. Suppose a Belgian prosecutor or investigative judge wishes to register (or order the registration of) incoming calls to a Belgian number on the basis of Article 88 *bis* Belgian CPC. They will not know in advance whether calls will come in from abroad and so be included on the list. In this case, there is a clear Belgian component and so there can be no objection with regard to the logging of foreign numbers.[128] If the prosecutor or investigative judge then wishes to identify the holders of these foreign telephone numbers (Article 46 *bis* Belgian CPC), this will have to be done through international legal assistance because he will require the help of a foreign entity that is not under his procedural jurisdiction. It is not because the telephone traffic can be labelled as (at least partially) "Belgian" that the request for identifying information on the foreign number might suddenly become a "purely Belgian" procedure.[129] The country borders have again become the borders to the exercise of jurisdiction. In the case of an order to cooperate, the decisive criterion is not, therefore, the location of the requested data[130], but the location of the subject from whom the prosecutor or examining magistrate seeks to obtain such data.
The same applies to "traditional" investigations, e.g. interview of a witness to a Belgian territorial offence that takes place abroad or the request of Swiss bank account details in a Belgian money laundering case. If someone transfers money, which is suspected to have illegal origin, to Belgium from a Swiss bank account, a money laundering investigation can be set up in Belgium and the transferred money seized. To interrogate the Swiss bank manager or obtain the identity of the holder of the Swiss account, the Belgian investigators must, however, ask Switzerland for legal assistance, no matter who holds the account or where the account holder resides.

33. OTHER ISSUES. - For the conscientious investigator, this conclusion will probably be quite disappointing. But we can turn it around. If Belgium allows its own people to conduct far-reaching, transborder, unilateral investigative work, then it must also, in view of the reciprocity principle, allow other States to do the same. While we might be able to live with this from our EU partners, it would be more difficult to accept that Chinese investigators were able to search the servers of Belgian companies with a territorial link to China, or that a Belgian social networking site such as Netlog was forced to disclose its information to the American government without Belgium being able to exercise any form of control. The company also risks getting into trouble due to non-fulfilment of the European data protection laws.[131]
This problem of issuing direct orders to foreign legal subjects actually dates from before the internet era. The practice is reminiscent of the American "discovery orders".[132] It consists in obliging US citizens, who fall within US jurisdiction, usually under the threat of a penalty (subpoena), to bring documents from abroad to the US.[133] The US sees this as an *indirect* territorial exercise of its jurisdiction because it does not itself conduct investigations in the foreign territory. Because the documents are brought to the US, the "discovery" is made on American territory. Therefore it shifts the border when it orders discoveries on

[126] "Foreign" because it is held by a legal subject based abroad, not "foreign" because the data are abroad.
[127] See, among others, G. HOSEIN, "International co-operation as a promise and a threat" in *Cybercrime and Jurisdiction. A Global Survey*, The Hague, T.M.C. Asser Press, 2006, 29 et seq.
[128] The masts used to send, forward and receive communication are distributed over various countries. The communication is received via Belgian masts, so there is a clear Belgian component. See B. DE SMET, "Registratie en lokalisatie van telecommunicatie" in *Strafrecht en strafvordering. Artikelsgewijze commentaar met overzicht van rechtspraak*, 28.
[129] Contrary to what the criminal court judge appears to be stating when he says that an international request for legal assistance was not necessary because the order related to the disclosure of data relating to the registration of Belgian territorial electronic traffic.
[130] And, moreover, unworkable in times of mobile internet, cloud computing and Wi-Fi. See also J. SPOENLE, "Cloud Computing and cybercrime investigations: Territoriality vs. the power of disposal?", Discussion Paper of 31 August 2010 and Draft Discussion Paper of 15 January 2010, "Law Enforcement Challenges in Transborder Acquisition of Electronic Evidence from 'Cloud Computing Providers'", www.coe.int/cybercrime (Project on Cybercrime).
[131] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, *Official Journal of the European Union - Legislation* 281, 23 November 1995, page 31; Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, *Official Journal of the European Union - Legislation* 350, 30 December 2008, p. 60; see also the proposal of 25 January 2012 for a new directive of the European Parliament and of the Council on the protection of private individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, COM/2012/010.
[132] See more on this in C. RYNGAERT, *Jurisdiction in International Law*, Oxford, Oxford University Press, 2008, 79-83.
[133] See, for example, *United States/Bank of Nova Scotia*, discussed by G. HOSEIN, "International co-operation as a promise and a threat" in *Cybercrime and Jurisdiction. A Global Survey*, The Hague, T.M.C. Asser Press, 2006, 37 and C. RYNGAERT, *Jurisdiction in International Law*, Oxford, Oxford University Press, 2008, 82.

foreign territory. However, the practice runs into systematic resistance from other States, particularly in Europe. Europe views the execution of this type of unilateral request without the permission of the other State as an intervention in the territorial sovereignty of that State. A typical example is the controversy surrounding the "Belgian" corporation Swift, which was intended to give the American authorities access to financial data.[134]
Therefore, America may not object too strongly to the case in question. A recent Council of Europe report shows that the same US Government uses such a practice in relation to cloud service providers falling under their jurisdiction. This is the case when the company or one of its subsidiaries is based in the US, but also when a company "*conducts continuous and systematic business in the United States*".[135] Because the US uses the practice itself, it might have no objection to unilateral orders against US private companies coming from Belgium. Then again, the practice does not tally with the traditional uncooperative European attitude to American orders for information. If Europe, with Belgium at its head, were to change track, it would be forced, in view of the reciprocity principle, to stop being uncooperative with these unilateral American orders, and this is something that the Americans would only applaud. RYNGAERT rightly concludes: "*Europeans may indeed reason that arguments of reciprocity counsel against unilateral assertions of jurisdiction in the field of the law of evidence. Although such assertions may confer short-term litigation benefits, such benefits may be outweighed by the burdens of future unilateral assertions of jurisdiction of other States.*"[136]
We should not lose sight of the fact that Belgian investigators might also run the risks of being prosecuted in other countries. Unilateral, trans-border tapping orders and network searches could be described in other States as unlawful eavesdropping and hacking.[137] As KASPERSEN rightly notes: "*Under public international law, there is no rule that law enforcement officers of one State can lawfully execute their duties as imposed by national law, nor can they invoke legal competences or coercive measures in that State as provided by their national law.*"[138]

34. "BITING" ABROAD. - When Belgium threatens foreign corporations with fines for non-fulfilment of a *unilateral* Belgian request for foreign evidence directed to a legal subject based abroad, it is exercising its power across its borders. In other words, this is a unilateral request with an extraterritorial effect. Therefore, it cannot be claimed that this is a purely territorial and domestic affair simply because the prosecutor has not physically left the territory of Belgium. The prosecutor's request is an order, a coercive measure (i.e. it carries criminal consequences - in this case prosecution - linked to refusal) and comes down to an extraterritorial exercise of Belgian criminal procedure. Without permission from the foreign government, an action of this kind is, in our opinion, contrary to international law.

3. Consequences for the offence in Article 46 bis, §2 Belgian CPC

35. EXCHANGE OF INFORMATION BETWEEN BELGIUM AND THE US. - What is the effect of a correct interpretation of the international law on the offence in Article 46 *bis*, §2 Belgian CPC? As of when was there a legal obligation that was not fulfilled? To answer this, we have to look at how legal assistance operates between Belgium and the United States. To exercise coercion on the American company Yahoo, the prosecutor should have honoured the legal assistance agreement. Belgium and the United States concluded a bilateral agreement on mutual legal assistance in criminal matters on 28 January 1988 (hereinafter the "MLAT").[139] This MLAT came into effect on 1 January 2000. According to Article 1, Belgium and the United States will

[134] Which eventually led to the agreement of 28 June 2010 between the European Union and the United States of America concerning the processing and disclosure of data in relation to the financial messages from the European Union to the United States as part of the terrorist finance tracking programme (TFTP agreement), *Official Journal of the European Union - Legislation* 195, 27 July 2010.
[135] CYBERCRIME CONVENTION COMMITTEE (T-CY), "Transborder access and jurisdiction: what are the options?", Report of the Transborder Group adopted by the T-CY on 6 December 2012, 48, www.coe.int/TCY.
[136] CYBERCRIME CONVENTION COMMITTEE (T-CY), "Transborder access and jurisdiction: what are the options?", Report of the Transborder Group adopted by the T-CY on 6 December 2012, 83, www.coe.int/TCY.
[137] See, for example, the American *Gorshkov and Ivanov* case in which FBI agents lured two Russian suspects to the US. The FBI gained access via the internet to Russian servers using the passwords they had obtained from the Russian suspects. Russia then accused the FBI agents of hacking. See, among others, N. SEITZ, "Transborder Search: A New Perspective in Law Enforcement?", *International Journal of Communications Law & Policy* 2004, issue 9, 1-18.
[138] H.W.K. KASPERSEN, "Jurisdiction in the Cybercrime Convention" in *Cybercrime and Jurisdiction. A Global Survey*, The Hague, T.M.C. Asser Press, 2006, 19. See also P.L. BELLIA, "Chasing Bits across Borders", *The University of Chicago Legal Forum* 2001, 35-101.
[139] Treaty of 28 January 1988 between the Kingdom of Belgium and the United States of America on mutual legal assistance in criminal matters, *Belgian Official Journal* 8 December 1999.

assist each other legally in all matters relating to the detection, prosecution and punishment of crime. The legal assistance relates to matters such as the location and identification of people (Article 1.2.a).[140]

Article 17 of the MLAT stipulates the procedure to be followed. All requests for legal assistance must be submitted and executed with the assistance of the central authorities. They maintain direct contact with each other with a view to implementing the provisions of the agreement. For Belgium, this is the Minister for Justice, his representative or his deputy. For the United States of America, this is the Attorney General or his appointed representatives.[141]

36. INTERPRETATION IN CONFORMITY WITH MLAT. - In this case, the prosecutor has not acted in accordance with Article 17 of the MLAT, but sent his request directly to Yahoo in the US. This has an effect on the offence in Article 46 *bis*, §2 Belgian CPC.

It means that the Belgian courts and tribunals must interpret national law in conformity with international law. For example, the International Court of Justice ruled against Belgium in the *Yerodia* case because the Belgian warrant for this man's arrest did not respect the criminal immunities under international common law.[142] By attempting to execute that arrest warrant around the world, Belgium was in violation of international law. The *Yerodia* judgement said nothing about the Belgian claim to substantive criminal jurisdiction in Yerodia's alleged crimes; it merely forbade the exercise of procedural criminal jurisdiction contrary to international law. Here, too, international law imposed limitations on the action of a magistrate prosecutor who was operating from a national framework. If the execution of an arrest warrant is contrary to international law and is not permissible, then neither is an order to cooperate or, a fortiori, a trans-border attempt to enforce it.
The Court of Cassation recognised this obligation of interpretation in conformity with international law in the *Sharon* judgement: "*Whereas, however, this rule of internal law would contravene the principle of customary international criminal law referred to above if it were to be interpreted as aiming to dismiss the immunity established by this principle; that the rule in question cannot therefore have this objective, but must be understood as excluding only a situation whereby the official capacity of a person leads to that person being considered irresponsible from a penal point of view for crimes relating to international law and set out by the law.*"[143]

An interpretation in conformity with the MLAT reduces the prosecutor's request for cooperation from Yahoo to an informal, obligation-free request. As we have already said, the MLAT would not prevent a direct, informal request for information from being sent and the addressee responding (see *supra*, no. 29). In this sense, we support the recent Court of Cassation judgement of 4 September 2012. The mere fact that the request was sent from Belgium to an address in a foreign country does not in itself *invalidate* the request. It is therefore a valid procedural action and Yahoo *can* respond. But it is not a coercive request to which Yahoo *must* respond.

A unilateral request of this type cannot be a coercive request, or order, because if it were, Belgium would be unilaterally exercising its sovereign power on US territory. To make it coercive, Belgium must make the request in conformity with Article 17 of the MLAT and the US must respond. To interpret Article 46 *bis*, §2 Belgian CPC in such a way as to compel a legal person based in a foreign country to bring information to Belgium upon simple request and on penalty of a fine is contrary to international law.
As a consequence, Yahoo has not (yet) committed a Belgian omission offence because there is not (yet) an obligation to respond to the "request" sent directly to their address.

37. WHAT IF…? - What if the court were to rule against Yahoo in the end (with or without legal assistance) on the grounds of Article 46 *bis*, §2 Belgian CPC? This would raise the question of the enforceability of the

[140] In the meantime the EU and the US have also agreed a legal assistance treaty (agreement of 25 June 2003 on mutual legal assistance in criminal matters between the European Union and the United States of America, *Official Journal of the European Union - Legislation* 181/34, 19 July 2003). This agreement led to an amendment of the Belgo-American Legal Assistance Treaty (coordinated by instrument, 16 December 2004, *Belgian Official Journal* 8 March 2010 (ed. 2), commencing on 1 February 2010).
[141] Since 2010, it has been possible to send requests for legal assistance using rapid communication techniques (including fax equipment or electronic mail). A formal confirmation must follow the request if this is required by the requested State (Article 17, §3 Legal Assistance Treaty).
[142] International Court of Justice 14 February 2002, Case concerning *the arrest warrant of 11 April 2000 (Democratic Republic of Congo/Belgium)*, *International Court of Justice Reports* 2002, 3.
[143] Court of Cassation 12 February 2003, *Pasicrisie Belge* 2003, I, 307, *Revue de jurisprudence de Liège, Mons et Bruxelles* 2003, 364.

penalty imposed, a fine in this case.[144] This is also a matter of jurisdiction to enforce. Therefore, the same international rules apply. In this case, the judgement would probably be no more than a paper tiger because Yahoo has no assets in Belgium and its execution could not be taken any further on Belgian territory.[145] To execute the penalty extraterritorially, Belgium requires the assistance of the American government. But we fear that the US will not offer much cooperation to the judgement.[146] RYNGAERT has described the situation eloquently in his thesis: *"If a person outside the territory does not abide by the norm prescribed extraterritorially, he could be sued in the territory of the enacting State. If he does not pay the fine, his assets in the territory could be seized. Similarly, he could be precluded from entering the territory or registering with a government agency. Thus, territorial enforcement jurisdiction could compel persons to comply with norms prescribed extraterritorially. When a person has no assets in the territory of the prescribing State and does not entertain contacts with that State, extraterritorial jurisdiction will ordinarily prove ineffective*."[147]

4. Need for international cooperation "2.0"

38. LEGAL ASSISTANCE UPDATE. - "Belgian" evidence need not necessarily be on Belgian territory, but it can be on foreign servers or held by foreign third parties, which quite easily makes modern evidence gathering very "multi-territorial" extraterritorial. So we see the development from uni- to multi-territoriality not only in the implementation of substantive criminal law, but also in criminal proceedings. But international law draws the line between the different sovereign legal orders and, when compared with the extraterritoriality of substantive criminal law, it seems more flexible than that of procedural criminal law. This gap is normally bridged by international legal assistance.[148] Why then, did the prosecutor not simply take the path of legal assistance? Probably because it is too cumbersome and slow. Belgium would have to explain the whole background of the case, everything would have to be officially translated, with the right stamps, signatures, etc. Also, a study of the practice reveals that the American authorities have often returned requests for legal assistance in the identification of users of electronic communication services without processing them.[149] Although the US is conventionally obliged to assist Belgium[150], this traditional legal assistance contains no mechanism by which to penalise the US or force it to act if assistance is not forthcoming or is too late. It is just not worth the effort for the average criminal case. Diplomatic pressure is the only possible solution, but we fear that Belgium will not really have much impact on the American authorities at that point.

It goes without saying then that increasing internationalisation and digitisation will increase pressure for flexible and efficient international cooperation.[151] For the time being, compromises are being sought, such as the aforementioned Article 20 of the EU agreement and Article 32 of the Convention on Cybercrime.[152] These two articles make legal assistance slightly more flexible, but they constitute an insufficient attempt to render the cooperation practical and efficient. For example, we see that Article

---

[144] Or the very surprising order for the "return" (Article 44 Belgian CC and 161 Belgian CPC) of the information under the penalty of a fine, following the criminal court judge in Dendermonde. Criminal Court of first Instance Dendermonde, 2 March 2009, *T. Strafr.* 2009, issue 2, 116, note.

[145] To remedy this "fault", the legislator could link the additional sanction in Article 36 Belgian CC (temporary or permanent ban on carrying out activities) to Article 46 *bis*, §2 Belgian CPC. Yahoo's site in Belgium could then be blocked. But it is debatable whether a block like this would be proportional and conformant with Article 10 of the ECHR. See ECHR, 18 December 2012, *Yildirim/Turkey*, no. 3111/10. See also Court of Justice, 16 February 2012, C-360/10, *Sabam/Netlog* and Court of Justice, 24 November 2011, C-70/10, *Scarlet/Sabam*. In these cases, the Court ruled that imposing a filtering system on an internet provider is inconsistent with the basic rights of the Union. The Court took into account the fact that this order could limit freedom of information because communication with legal content could also be blocked.

[146] See the French-American *Yahoo* case in which the American judge refused to implement a French judgement in the US because it was inconsistent with the American right to freedom of speech (*Yahoo! Inc./La Ligue Contre Le Racisme et L'Antisemitisme*, 169F. Supp. 2d 1181, 1192). M. SADAAT, "Jurisdiction and the Internet after Gutnick and Yahoo!", *Journal of Information, Law and Technology* 2005, 20-21 (http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2005_1/saadat/); E. SCHEFFEL, "Court refuses to enforce French order attempting to regulate speech occurring simultaneously in the U.S. and in France", *Computer & High Technology Law Journal* 2003, 549- 558.

[147] C. RYNGAERT, *Jurisdiction in International Law*, Oxford, Oxford University Press, 2008, 24-25.

[148] P.L. BELLIA, "Chasing Bits across Borders", *The University of Chicago Legal Forum* 2001, 44.

[149] Unless it involves terrorism, international drug or arms trading, or there is a proven American interest in the request (e.g. linked to a current American case file or concerning an American citizen).

[150] See also G. HOSEIN, "International co-operation as a promise and a threat" in *Cybercrime and Jurisdiction. A Global Survey*, The Hague, T.M.C. Asser Press, 2006, 34-35.

[151] See also M.A. SUSSMAN, "The Critical Challenges from International High-Tech and Computer-related Crime at the Millennium", *Duke Journal of Comparative & International Law* 1999, issue 9, 468 et seq.

[152] H.W.K. KASPERSEN, "Jurisdiction in the Cybercrime Convention" in *Cybercrime and Jurisdiction. A Global Survey*, The Hague, T.M.C. Asser Press, 2006, 20.

32 of the Convention on Cybercrime is much stricter on transborder network searches than its counterpart provision, in relation to the trans-border tap, in the EU's Convention on Mutual Assistance. This is because the EU States tend to go for intra-EU transborder cooperation.
But even the provision of Article 20 of the EU Convention applies only when there is no need for active cooperation from foreign intermediaries. This shows that the Parties to the Convention considered it a step too far to allow States unilaterally to coerce foreign IT-intermediaries to cooperate, which Belgium undeniably tried to do in the *Yahoo* case.
Other compromises in the Convention on Cybercrime are, for the time being, the expedited preservation measure (Article 29), the expedited disclosure measure (Article 30) and the setup of permanent points of contact (Article 35). These measures should relieve the problems relating to the speed and transience of electronic communication to a certain extent and prevent States from acting on their own initiative. On the basis of Article 29, a State can request that another State impose an expedited preservation of stored computer data on its legal subject. The requesting State must then, however, send a legal assistance request in order to obtain these data.[153] There is one important exception to this. Article 30 stipulates that if, when implementing a request made under Article 29, the requested State discovers that a service provider in another State was involved in transmission of the electronic communication, the requested State must provide the requesting State with the necessary "traffic data" as soon as possible[154] so that this service provider and the path through which communication was transmitted can be identified.[155] The combination of these two articles therefore appears to solve (at least on a theoretical level) the prosecutor's problem in this case and enables, more generally, a faster acquisition of the data held by service providers based abroad. The procedure sounds great in theory, but in practice appears to run into the same problems experienced with traditional mutual legal assistance. Implementation of the measure may yet be too slow to allow the capturing of the needed data[156], and the willingness of some States to cooperate with requests of this type is often limited.
It is to be hoped that Article 35 will satisfy the high expectations of those who look for better cooperation. This article stipulates that States establish a point of contact that is to be continually available and guarantees immediate assistance, among other things for the location of suspects.[157] The setup of a 24/7 network of this type is, in our opinion, one of the most important achievements of the Convention on Cybercrime. The long-awaited ratification of the Convention on Cybercrime by Belgium offers new prospects for an advancement of legal assistance.

39. THE "POWER OF DISPOSAL" - As we have said, the Council of Europe is currently considering amendments to Article 32 of the Convention on Cybercrime. The report by the Cybercrime Convention Committee gives several interesting suggestions to "update" trans-border access to data.[158] Of the policy options under consideration, we think that the suggestion to replace the location of the data as a condition for procedural criminal jurisdiction with "the power of disposal" is a deserving one. It binds the data to the person or people who have the right to access and "administer" them (edit, delete, deny others the right of access and use, etc.). For these data to fall under the jurisdiction of the investigating State, this "administrator" would have to physically be in the territory of the investigating State or be a national subject.[159] This new criterion offers prospects for transborder network searches but not for coercive orders issued to foreign service-providers. When the latter is the case, it is not the place where the data are

[153] Explanatory Report to the Cybercrime Convention, §283 and 284: "*At the same time, a requested party is permitted to use other procedures for ensuring the rapid preservation of data, including the expedited issuance and execution of a production order or search warrant for the data. The key requirement is to have an extremely rapid process in place to prevent the data from being irretrievably lost. (…) Finally the requesting Party must undertake to subsequently submit a request for mutual assistance so that it may obtain the production of the data*."
[154] Article 1, (d) of the Cybercrime Convention states that this includes data relating to the origin of the communication (IP addresses, numbers, etc.). See Explanatory Report to the Cybercrime Convention, §30.
[155] See Explanatory Report to the Cybercrime Convention, §290: "*In doing so, the requested Party may discover that the traffic data found in its territory reveals that the transmission had been routed from a service provider in a third State, or from a provider in the requesting State itself.*" For example, if the data lead back to the requesting State itself, it can obtain the necessary information through internal measures. If they lead back to a third State, the requesting State can again make an expedited preservation or expedited disclosure request, this time to the third State.
[156] H.W.K. KASPERSEN, "Cybercrime and Internet jurisdiction (Draft discussion paper prepared in the framework of the Project on Cybercrime of the Council of Europe)", 28, www.coe.int/cybercrime.
[157] States can themselves choose who to appoint. For Belgium, it is the Federal Computer Crime Unit (FCCU). See Explanatory Report to the Cybercrime Convention, §298.
[158] The scope of the present contribution does not allow us to go into this in any more detail. See the report of the CYBERCRIME CONVENTION COMMITTEE (T-CY), "Transborder access and jurisdiction: what are the options?", Report of the Transborder Group adopted by the T-CY on 6 December 2012, www.coe.int/TCY.
[159] J. SPOENLE, "Cloud Computing and cybercrime investigations: Territoriality vs. the power of disposal?", Discussion Paper of 31 August 2010, www.coe.int/cybercrime.

stored that should be relevant, but the place where the person charged with the duty to cooperate (the "administrator") is located (see *supra* no. 32).
Unfortunately, the report pays little attention to the problems posed by *Yahoo*-like cases (transborder request instead of transborder access). It merely states that when data are in the hands of a service provider in a foreign country, the investigating authorities must generally take the path of legal assistance. However, they will experience technical and legal difficulties in this regard. Some States do allow service providers to respond directly to requests from foreign law enforcement authorities. Under some circumstances, information might be voluntarily exchanged.[160]
The time has come to find an international generally agreed solution to this problem. With the right guarantees, it might be possible, for example, to oblige service providers to respond to requests to disclose identification data to foreign law enforcement authorities, provided that data has links with the territory of the investigating State, such as the suspect or victim is a national subject of that State.[161] In this case, the data is identification information relating to electronic communications. Those communications were generated for the most part in the investigating State, and use was made of internet access and/or service providers based in that State. The role of the foreign service provider was merely secondary, the communication had its centre of gravity in the investigating State.
Just as the US first negotiated an agreement with Belgium and then with the EU over more rapid American access to financial data of the type held by companies like Swift in its fight against terrorism, it would seem recommendable that the US oblige its internet companies to comply directly with requests for user information coming from judicial authorities from EU-states or the EU as such. It would be desirable, of course, to have a standardised electronic communication system for this, which could guarantee speed, authenticity and confidentiality. In more sensitive cases, such as when the request could endanger relevant interests (e.g. medical confidentiality, professional secrecy, business confidentiality or other national interests), the US government could then intervene.

V. Conclusion

40. BARKING DOGS CAN AWAKE POLICYMAKERS. - The channels of traditional international legal assistance are too slow to be suited for cyber-investigations. In the *Yahoo* case, the prosecutor attempted to circumvent the inadequate system of legal assistance in cybercrime cases by subjecting a foreign service provider to unilateral Belgian authority via the offence provided for in Article 46 *bis*, §2 Belgian CPC. In our opinion, the decision was wrong, or, as the Americans would say, the prosecutor was "barking up the wrong tree". The broad substantive reach of the Belgian duty to cooperate does not, in our opinion, present an international legal problem, and Belgium can use its criminal law to enforce that duty. It is wrong, however, to employ this offence in order to obtain foreign evidence without respecting the international rules. The broad geographical scope of substantive criminal law cannot, in other words, lead to a breach of the more strict rules of international law when it comes to the actual cross-border enforcement of national laws. Unlike the, we do not consider the case at hand to be a purely Belgian territorial matter which Belgium can resolve on a unilateral basis. Belgium, or better yet the EU, should first take international initiatives to speed up the legal assistance process. The *Yahoo* case illustrates all the more clearly how pressing the need for workable instruments in the digital context is. It is to be hoped that, through his actions, Belgium's "barking Pac-Man" has finally woken up the powers that be, which should urgently develop the much needed legal assistance "2.0".

[160] CYBERCRIME CONVENTION COMMITTEE (T-CY), "Transborder access and jurisdiction: what are the options?", Report of the Transborder Group adopted by the T-CY on 6 December 2012, 31 and 44, www.coe.int/TCY.
[161] As in this case, the communication had a Belgian-territorial component. See also the reasoning of the criminal court judge, Criminal Court of Dendermonde, 2 March 2009, *T. Strafr.* 2009, issue 2, 121. We refer in this matter to the current doctoral dissertation by Lewis Chezan Bande at KU Leuven entitled "Cross-Border Access to Computer Data by Foreign Law Enforcement and the Position of Private Actors: Reducing the Role of Requested-State Authorities in International Cooperation against Cybercrime?".

b-ccentre

In collaboration with our academic partners

icri

Institute of Criminal Law

KU LEUVEN

UNIVERSITÉ DE NAMUR

crids
CENTRE DE RECHERCHE INFORMATION, DROIT ET SOCIÉTÉ

www.b-ccentre.be

@B_CCENTRE